HACKER JOURNAL

Anno 2 - N. 38
20 Novembre - 4 Dicembre 2003

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
grand@hackerjournal.it, Il Coccia, Gualtiero Bismark.it, Tronconi, Ana Esteban, Marco Bianchi, Edoardo Bracaglia, Polao Capobussi, Lucio Bragagnolo, Amedeu Bruguès, Gregory Peron

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Roto 2000

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601. Direttore responsabile - Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE
Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. **redazione@hackerjournal.it**

hack·er (hăk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

HACK'N'ROLL

Da questo mese viene pubblicata anche in Italia la rivista Rolling Stone, probabilmente la più antica e importante pubblicazione Rock americana. A sfogliarla, però, non si può non avere una sensazione strana. La parte editoriale prende; in molte parti è ruvida come dovrebbe. La pubblicità, invece, è quella che ci si aspetta di trovare in una rivista da parrucchiere maschile di tendenza: stilisti, profumi, auto di lusso e un po' di gagdet hi-tech.

Non so voi, ma quando vado a un concerto, l'unica mia preoccupazione in fatto di vestiti è che non deve dispiacermi troppo se i pantaloni si macchiano di fango fino alla cintura, o se la maglietta si strappa mentre sto pogando. E le scarpe devono essere abbastanza comode da farmi stare in piedi finché ne ho voglia.

Insomma, in bocca rimane uno strano sapore metallico addolcito da troppo miele, una specie di incongruenza, una contraddizione di fondo. Che traspare anche da alcune pubblicità. Una di queste mi ha colpito in particolare. Una pagina del super gestore Telefonico Italiano che pubblicizzava il suo servizio Adsl ricaricabile (che qui chiamerò celiA). Il titolo cerca di stare a suo agio sulla rivista: "Card Rock", e la frase a effetto non è da meno: "Non senti altro che MP3? Usa l'Adsl quando ce n'è un buon motivo".

Ora, avete anche voi la sensazione che una grande azienda multinazionale sta cercando di stimolare i suoi potenziali clienti ad acquistare un suo servizio per compiere un'azione quanto meno discutibile?

Altre multinazionali non si trovano in una situazione migliore: c'è un colosso dell'elettronica che ha anche varie etichette discografiche (visto che sono in vena, lo chiamerò Nyso), e mentre una sua mano produce dischi e si batte con tutti i mezzi perché non vengano copiati, prestati, ascoltati da più di cinque persone eccetera, con l'altra mano produce e vende masterizzatori e supporti di ogni tipo.

La cultura Rock e quella dell'hacking hanno molto in comune: quel senso di appartenenza a una comunità, il gusto per per l'estremo, le sfide ai margini della legalità, e un sano senso di ribellione. E anche dalle nostre parti c'è qualcuno pronto a usare questi elementi per guadagnarci.

Stanno infatti cominciando a sorgere aziende che dicono di praticare l'"hacking etico" per cavalcare un filone che ora va di moda, ma con l'hacking non hanno nulla a che fare. Oltre ovviamente alle altre aziende di sicurezza tradizionali, per le quali l'hacker è solo uno spauracchio da agitare davanti ai clienti per terrorizzarli e vendergli i suoi prodotti.

L'argomento è complesso, delicato, e non può esaurirsi in mezza paginetta. Ne parliamo infatti nell'articolo alle pagine 10-13, tenendo ben presente anche che accanto a questi, ci sono anche alcuni hacker che hanno sfruttato le proprie conoscenze per inventarsi un lavoro senza per questo abbandonare lo spirito originale, e infatti continuano a rendere disponibili i propri software e i propri studi.

grand@hackerjournal.it

PS: in ogni caso, benvenuta Rolling Stone ;-)

freeHACKnet

Saremo di nuovo in edicola Giovedì 4 dicembre !

HACKER JOURNAL

La prima rivista hacking italiana

2€ NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

>> IL TUO ACCOUNT | >> FORUM | >> DOWNLOADS | >>

HJ DOWNLOAD

Sapevate che hackerjournal.it c'è anche una sezione che elenca e recensisce i migliori software e strumenti di sicurezza? La "collezione" è in continua crescita, anche perché siete voi a costruirla, aggiungendo le vostre segnalazioni e recensioni. Al momento, sono elencati più di 110 programmi, suddivisi in nove categorie:

- Anti-Troyan
- Antivirus
- Firewall
- Forensic Tools
- Intrusion Detection
- Linux
- Scanner
- Stress Testing Tools
- Windows



Fateci un giro: scommettiamo che molti programmi non li conoscevate ancora?

I vostri siti...



www.secureitaly.org



http://web.tiscali.it/no-redirect-tiscali/juniord2003

freeHACKnet

freeHACKnet è il servizio gratuito di collegamento a Internet targato Hacker Journal: indirizzo email @hackerjournal.it con 5 Mbyte, accesso super veloce fino a 128 Kbit al secondo (ISDN multilink PPP), server newsgroup, controllo anti virus e anti spam. Niente abbonamento, nessuno sbattimento, paghi solo la tariffa telefonica urbana.
Corri subito a iscriverti su
www.hackerjournal.it/freeinternet

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete gli arretrati, informazioni e approfondimenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo!

user: sball8
pass: ex3mis

HACKER JOURNAL

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

mailto:
redazione@hackerjournal.it

LICENZE PER SCRITTI E RACCONTI

Sto lavorando alla realizzazione di un progetto in cui tutti possano pubblicare i propri libri e racconti di qualsiasi genere essi siano, spaziando dalla letteratura all'informatica. Per fare questo c'è bisogno di una licenza che tuteli quelli scritti.... Cosa devo fare??

phj

In Italia ogni opera letteraria è protetta in modo automatico: non occorre apporre una dicitura di copyright; basta poter dimostrare di esserne l'autore. Certo, l'apposizione di un copyright che indichi in modo esplicito l'autore e l'anno di produzione è un ulteriore avvertimento a chi intenda appropriarsi dell'opera.
Detto ciò, si possono scegliere anche forme di licenza che consentano per esempio la libera copia e successiva diffusione dell'opera, pur mantenendone i diritti d'autore. In questo senso, le formule più interessanti e utilizzate sono la Free Documentation License di GNU (www.gnu.org) e quelle proposte da Creative Commons (www.creativecommons.org). Nota comunque che anche queste licenze sono una forma di copyright. Fatte queste considerazioni, se il progetto è molto importante, consulterei comunque un avvocato specializzato sulla tematica del diritto d'autore, che ti può dare consigli molto più adatti alla situazione italiana.

VIRUS VIA SMS



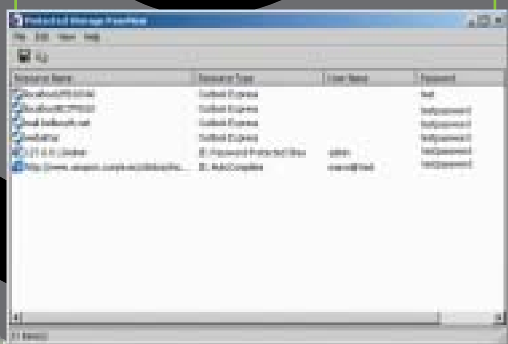
Leggevo sul numero 35 di HJ, nell'articolo che parla dei trucchi per cellulari, che esistono anche dei virus per siemens, che possono essere inviati via sms (non avrei mai pensato che si sarebbe arrivati anche a questo). Per questo motivo, da un pò di giorni, mi sto chiedendo come sia possibile che tramite un sms si possa mandare in crash un cellulare. Mi piacerebbe poter leggere qualcosa riguardo questa logica. Come sia possibile intaccare il SW di un celluarle tramite SMS. Forse porprio tramite i comandi AT? Vi ringrazio moltissimo per quanto farete per colmare questa mia curiosità e se dovessi essere anche di spunto per un vostro articolo, beh... ne sarei veramente molto onorato.
Grazie ancora e complimentissimi per la vostra rivista.

Il PrincipeLele

Le basi tecniche sono le stesse che consentono di aggiungere, per esempio, un nuovo logo o una suoneria tramite un SMS. In entrambi questi casi, il contenuto degli SMS viene scritto in certe aree della memoria del telefono. Se al posto di un logo c'è del codice malevolo, e se si fa in modo che questo venga scritto in zone di memoria in cui non bisognerebbe ficcare il naso, ecco assicurato il crash del cellulare.

RECUPERARE PASSWORD DI POSTA

Alcuni miei colleghi hanno fatto un po' di pasticci con dei PC della scuola in cui lavoro. Nella loro imperizia, ultimamente hanno cancellato le password di accesso



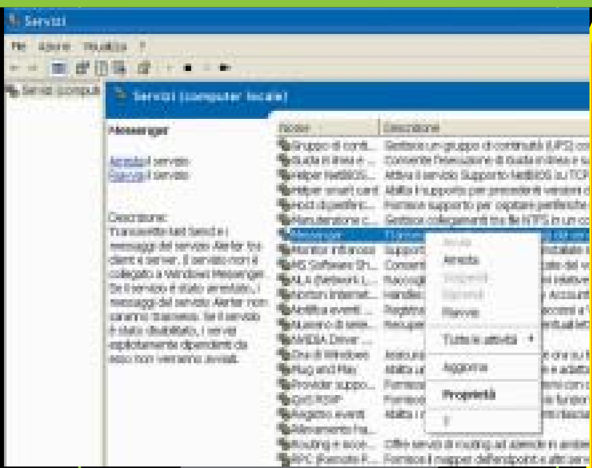
agli account di posta elettronica. Teoricamente non ci sarebbero dovuti essere molti problemi, perche' le iscrizioni sono state tutte stampate, registrate in segreteria e protocollate, ma la segreteria ne ha perse due! Tutte le altre verranno ripristinate, ma queste due, fra l'altro abbastanza importanti sembrano perse per sempre.
Mi ricordo pero' che anni fa, davanti a un problema simile, su una rivista specializzata trovai indicazioni su come raggiungere un file di registro nel quale erano memorizzate le pwd. Naturalmente non ho piu' le preziose informazioni e non mi ricordo se si riferiscono anche agli account di posta.

Maria Grazia P.

Un tentativo si può fare con alcuni programmi che però, nella maggior parte dei casi, possono operare solo se la password è ancora registrata dal programma (cioè, se si possono vedere gli asterischi che mascherano il campo della password).
Una raccolta di programmi gratuiti è disponibile su www.webattack.com/freeware/security/fwpasswordrecovery.html.
Se la password è stata però cancellata dal computer, non c'è molto da fare. Ogni tentativo di "indovinare" la password agendo sul server di posta con strumenti di attacco a forza bruta (che provano ogni combinazione di caratteri), possono essere interpretati come un attacco informatico punibile penalmente, anche se gli attacchi sono rivolti ad aprire la propria casella di posta.
Il traffico e le richieste generate da questi programmi assorbe molte risorse del server del provider, che può ritenersi "parte lesa".
In questo secondo caso, l'unica strada percorribile è quella di rivolgersi al provider stesso, che è senz'altro in grado di impostare una nuova password.
Auguri per le inevitabili attese in linea con il supporto tecnico del provider :-/

SPAM ISTANTANEO

Carissima direzione di HJ volevo chiedere a voi, che siete molto impegnati da sempre nella lotta contro lo spam come faccio a chiudre una volta per tutte tutte quelle fastidiossissime finestre pubblicitarie che si aprono durante la navigazione su internet:gli "about:blank" io non penso che sia pubblicità "normale" cioè quella che supportano un sito e che si aprono



quando si visita un sito,infatti se resto collegato ad internet (anche se non apro Internet Explorer) mi si aprono lo stesso e un altro effetto collaterale è che rallentano la connessione essendo la mia una 56K dial up resto nelle vostre mani

Consoman89

Hai ragione: non si tratta di una pubblicità normale, ma di quello che viene definito "Spam del servizio Messenger". Windows XP e Windows 2000 hanno abilitato un servizio che consente di ricevere messaggi che compaiono sullo schermo all'interno di una finestrella. Lo scopo di questo servizio è quello di consentire all'amministratore di una rete di mandare messaggi urgenti a tutti gli utenti (per esempio, per avvisarli dell'imminente spegnimento del server). Il servizio però non è soggetto ad alcuna autenticazione efficace, per cui chiunque può inviarti un messaggio semplicemente conoscendo il tuo indirizzo IP (o, più facilmente, sparando indirizzi IP a caso).
Per evitare il problema, devi disabilitare il servizio messenger (occhio, non c'entra nulla con MSN Messenger, il programma di messaggistica istantanea). Per fare ciò, su Windows XP, lancia il programma "services.msc" (da Start/Esegui). Nella lista "Servizi" individua la voce "Messenger", fai clic col pulsante destro del mouse su di essa e seleziona "Arresta". Su Windows 2000, la lista dei servizi si trova in Pannello di Controllo/Strumenti di Amministrazione.

ALCUNE PRECISAZIONI...

Salve redazione di hj, sono un lettore della vostra rivista. Vi scrivo per informarvi che nel numero 36 a pagina 27 c'è un po' di confusione nell'uso di '>' nella shell di linux. Nella seconda colonna della pagina si legge: "L'ultimo operatore che analizzeremo è >: esso svolge una funzione analoga all'operatore > ma si preoccupa...". Potrebbe essere solo un errore di stampa: infatti l'operatore che appende ad un file già esistente l'output di un comando è >> e non >. La svista è ripetuta anche nel riquadro verde.

Stefano

Più che un errore di stampa: è un errore di sviluppo! Per applicare gli stili al testo che sarà importato dal programma usato per l'impaginazione (Quark XPress), usiamo un programmino che ci siamo sviluppati da soli in redazione, e che inserisce automaticamente i tag usati per applicare gli stili. Come nell'html, questi tag si aprono e si chiudono coi segni di maggiore e minore. Prima di applicare gli stili, il nostro programmino ovviamente sostituisce i simboli di maggiore e minore nel loro tag equivalente (altrimenti incasinerebbero l'apertura e la chiusura dei tag degli stili). Quello che non abbiamo previsto è la presenza di due segni di maggiore o minore consecutivi: in questo caso, infatti, il primo segno viene convertito, il secondo viene invece "perso per strada". Purtroppo non ci siamo accorti dell'errore in fase di revisione delle bozze.

CLONECD È MORTO: SI PUÒ CRACCARE?

Come probabilmente saprete, (http://www.elby.ch/it/products/clone_cd/index.html), la Elaborate Bytes ha dovuto cessare la vendita di CloneCD dato che superava agevolmente le protezioni CD. Ora che succede? Non più diritto fare copie di backup?
Io avevo scaricato già la trial di CloneCD, ma ora è scaduta: il software ha perso anche il copright? se clicco su acquista key mi dice che il soft non esite più, di conseguenza posso cracckrlo senza problemi legali? Oppure, nonostante abbia perso anche il copright, ora è illegale anche USARE il software già scaricato?

Brutti tempi per i cloni... la pecora Dolly è morta, CloneCD non si può più vendere, e prima o poi qualcuno si accorgerà anche di Zucchero. Dunque, le problematiche sono varie e separate tra loro.
Elaborate Bytes non può più vendere CloneCD perché viola una legge americana. Questo non ha ripercussioni sugli utenti italiani che hanno già acquistato il programma, che possono ancora duplicare CD audio allo scopo di creare una copia di sicurezza personale.



Il fatto che il software non sia più in vendita non fa però decadere i diritti di autore, che continuano ad appartenere a Elaborate Bytes. Ora, sebbene in Italia tu possa usare legalmente CloneCD, non lo puoi copiare o craccare, perché (questo sì), in Italia è un reato. Chi non ha acquistato in precedenza una copia di CloneCD, non potrà quindi usarlo.

NEWS



HOT!

GLI OCCHI A MANDORLA DELLA CENSURA



Il Grande Fratello del Ministero della Cultura cinese ha puntato il suo occhio inquisitore sugli Internet Cafè della nazione. Non solo tutti i punti di accesso pubblico alla Rete saranno obbligati a installare software di controllo per monitorare le attività dei clienti. Pare anche che la licenza di apertura di esercizi verrà d'ora in poi concessa esclusivamente a grandi catene controllate dallo Stato. La situazione incresciosa è stata denunciata da Reporter Senza Frontiere (http://www.rsf.org/), organizzazione che da anni si batte per la libertà di informazione nel mondo.

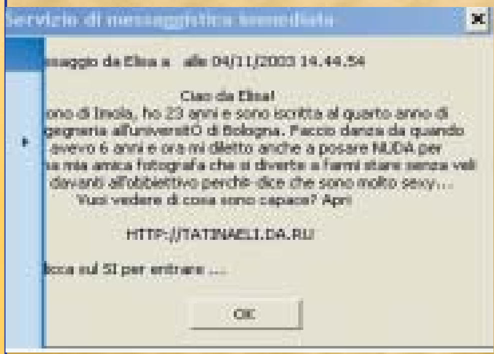
LINEA DURA PER TELIA



Telia, uno dei più grandi Internet Service Providers svedesi ha deciso di bloccare i computer di tutti coloro che inviano spamming tramite i suoi server. I computer bloccati principalmente sono quelli infestati da trojans che spediscono all'impazzata centinaia di messaggi indesiderati. Immaginiamo la gioia degli utenti: infetti e mazziati, ehm… inchiodati. Telia assicura comunque di offrire assistenza ai malcapitati, aiutandoli a rimuovere il problema il più velocemente possibile.

MA…CHIEDERE IL PERMESSO?

La botta di iniziativa di AOL ha lasciato tutti quanti stupefatti e parecchio contrariati. Senza minimamente interpellare i suoi abbonati, il colosso americano ha infatti deciso di disabilitare Windows Messenger. Il servizio, che nulla ha a che vedere con il client di



messaggistica istantanea, è vero, costituiva un canale privilegiato per lo spamming, nonché un punto di possibile vulnerabilità per il sistema. Ma non si capisce come AOL si possa essere presa tale ingiustificata e ingiustificabile libertà. Libertà che, diciamocela tutta, a un ragazzino o hacker qualunque sarebbe costata indagini, diffide, sanzioni e quant'altro. AOL si difende dalle accuse come niente fosse, dicendo che il servizio è per lo più sconosciuto agli utenti, che è riattivabile con un clic del mouse e che ha avuto accordi sulla faccenda con il big di Redmond. Animata da tante buone intenzioni, forse AOL non si rende conto del paradosso. Combattere l'intrusione con… un'intrusione non richiesta. Ma del resto c'è anche chi pensa di fermare le guerre con altre guerre. Deve essere così che va il mondo.

TRENI DEL FUTURO DISAGI DEL PRESENTE?

Carrozze attrezzate per connessioni wi-fi, passeggeri mollemente adagiati che ingannano il tempo guardando la TV on demand, alacri omini incravattati che trasformano il viaggio in treno in un'occasione per lavorare ancora di più e meglio. Ma dove siamo? In un film ambientato nel futuro o tra i fotogrammi dell'incubo di un qualche manager malato di efficientismo e di tecnologismo? Macchè. Siamo a Genova dove pochi giorni fa Trenitalia ha presentato un nuovo modello di treno del futuro. Il progetto si chiama Fifth (Fast Internet For Fast Train Host), è realizzato in collaborazione con Alenia Spazio e prevede l'allestimento di spazi tecnologicamente attrezzati sui treni di lunga percorrenza. Le sperimentazioni avranno luogo per tutto il 2004 su treni speciali. Dall'anno successivo i servizi saranno disponibili sugli Eurostar ed entro il 2005 anche sugli Intercity. Che dire, siamo fieri di essere italiani, di essere al passo con l'Europa e di essere promotori di servizi tanto



all'avanguardia. Anche se qualche volta ci basterebbe che i convogli di Trenitalia giungessero puntuali, non imballati come una discoteca la notte di capodanno, non ammorbati e appiccicosi come la stessa discoteca la mattina dopo, che fossero tiepidi d'inverno e almeno un po' freschi d'estate. È chiedere troppo?

A OGNUNO LA SUA PROTEZIONE

I bambini si sa, hanno l'occhio lungo e a volte curiosità un po' troppo pruriginose per la loro giovane età. Per i genitori preoccupati della sicurezza online dei loro figli, Telecom lancia Alice Family. Si tratta di un'offerta di abbonamento ADSL che prevede quattro caselle di posta e quattro accessi alla Rete indipendenti. Grazie a Parental Control, ogni accesso potrà collegarsi a Internet con un diverso grado di protezione, tutelando così i più piccoli da visioni e contenuti non adatti, anche quando mamma e papà non sono in casa. Fino al 31 dicembre l'attivazione di Alice Family sarà gratuita. Dopo di che costerà 2 euro al bimestre.

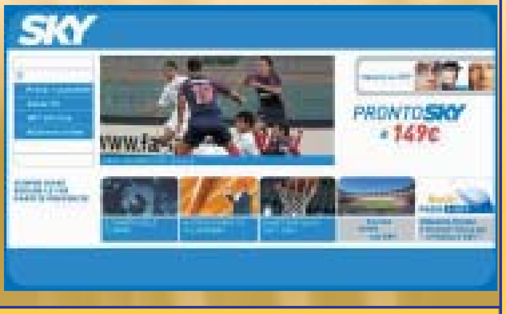


Per informazioni: www.aliceadsl.it.

HOT!

MA GUARDA CHE SORPRESA

Metti un giorno di essere online sulla tua scheda abbonato Sky,. Metti di essere annoiato e di cincischiare con i numerelli dell'url. Metti che, cambia una cifra qua e una là, e guarda un po' cosa accade. Ti si visualizza in tutto il suo splendore la scheda di un altro abbonato. Con tanto di nome, cognome, indirizzo e dati personali. Sembra impossibile, dato che i server di Sky sono di tipo sicuro. Eppure è successo ad alcune persone che poi hanno segnalato l'accaduto a Punto Informatico. Per fortuna la pagina Web che permette questo tipo di accesso non è facilmente raggiungibile dal sito dell'operatore satellitare. Il problema risiede infatti in una macchina di servizio utilizzata dalla rete di dealer Sky e non del server dove si trova il sito dell'operatore. Sky è stata avvertita, dunque si suppone che a breve di questo imbarazzante inconveniente non vi sia più traccia.



OPERAZIONE CATARTICA



Sì, la buona riuscita dell'operazione della guardia di finanza contro il worm Zelig è stata una sorta di purificazione liberatoria. Soprattutto per i portafogli a rischio di molti internettari. Nei giorni tra il 24 e il 25 ottobre scorsi, si è diffuso un messaggio di posta elettronica apparentemente innocuo che invitava a visitare un sito dove avremmo trovato un salvaschermo con "messaggi catartici", le ormai note perle di saggezza di Flavio Oreglio di Zelig. Una volta raggiunta la home page indicata, avviare il download era un attimo. Inutile dire che si trattava di una truffa che dirottava la nostra connessione telefonica su un numero da 1,80 euro al minuto. Per fortuna il pericolo è scampato. L'organizzatore della truffa, un commerciante di pelli di Pisa domiciliato a Caracas, è già stato fermato dalle forze dell'ordine. Stiano tranquilli tutti coloro che hanno ceduto alla tentazione del clic. Grazie al tempestivo intervento della GdF, non riceveranno le tanto temute, e per nulla catartiche, bollette astronomiche.

ALLO SPAMMER! ALLO SPAMMER!

Le vie dello spamming sono davvero infinite. Gira voce che cominci a diffondersi questa piaga anche via Bluetooth. Il fenomeno si chiama bluejacking e per ora sembra sia soltanto la bravata di qualche buontempone. Ma non fatichiamo pensare che spammers seri prima o poi possano approfittare della possibilità di inviare messaggi via Bluetooth tra dispositivi accesi nel raggio di pochi metri . Ci immaginiamo eserciti di mercenari, che travestiti da uomini d'affari sparano messaggi indesiderati, sui treni, in metropolitana, alla stazione, negli uffici. Che succederà a quel punto? Diffidentissimi, copriremo telefoni, computer e palmari con gli astucci, come quando a scuola non volevamo ci copiassero. E al minimo sospetto urleremo impalcabili "allo spammer! allo spammer! prendetelo!".



C'È SEMPRE UNA PRIMA VOLTA



La prima volta non si scorda mai. Anche quando si tratta di vincere una causa anti spam. Per la California l'evento è di qualche giorno fa. La causa è costata ben due milioni di dollari di multa a una azienda di marketing che ha inviato milioni di mail non richieste. Nei messaggi si trovavano consigli su come realizzare mail pubblicitarie e una quantità spropositata di indirizzi di posta elettronica. Oltre ricevere la multa, i responsabili dell'operazione marketing sono stati diffidati dal gestire e amministrare affari che riguardino la pubblicità in Rete per i prossimi dieci anni.

OPEN SOURCE NO PROBLEM

Le Amministrazioni pubbliche che vogliono passare da software proprietari a software open source, prendano nota del sito dell'Unione Europea, http://europa.eu.int. Qui si trovano informazioni sui diversi prodotti open source e una tabella per calcolare quanto si risparmia passando da una formula all'altra. Il documento, redatto da esperti nel settore di tutta Europa, è costantemente aggiornato.

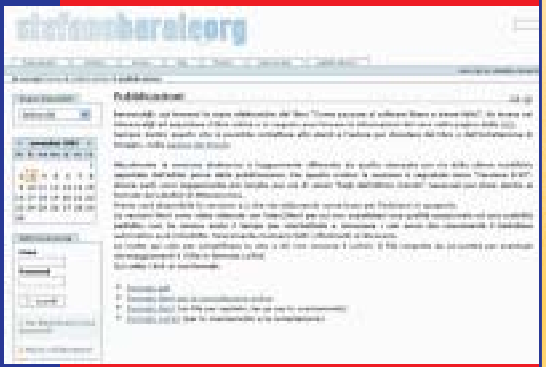
LA VERITÀ È VICINA

POLIZIA di Stato

Si è finalmente aperta l'inchiesta della Polizia Postale e delle Comunicazioni sulla truffa anti eBay. Il raggiro riguarda un messaggio fasullo che cerca di convincere gli iscritti a eBay a inviare i dati personali, compresi quelli della carta di credito. Al momento le indagini sono ancora in corso e non si sa né chi abbia architettato il piano, né quante persone siano cadute nella trappola dei truffatori. Naturalmente eBay è assolutamente estranea alla faccenda. Anzi, ricorda che non avrebbe ragione alcuna di richiedere informazioni del genere ai suoi iscritti.

HOT!

PER SAPERNE DI PIÙ



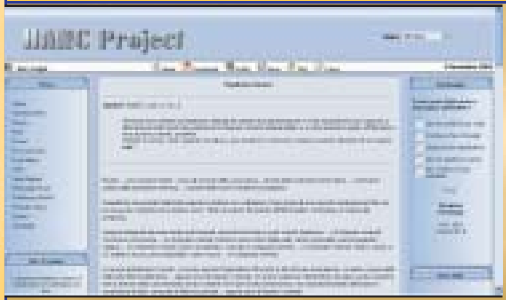
Se ancora l'open source non ci ha convinti del tutto e aspettiamo quell'argomentazione in più per liberarci dai vincoli del software proprietario, proviamo a dare un'occhiata a questo libro. Costa 10 Euro e si chiama "Come passare al software libero e vivere felici - Manuale di autoliberazione informatica". Tra le sue pagine troveremo non solo teoria ma anche tanta pratica e spiegazioni tecniche. Sul sito dell'autore, www.stefanobarale.org è disponibile anche la versione elettronica della pubblicazione.

MCDONALD'S CONNECTION

Nessuno resiste più alla voglia di wi-fi, nemmeno Mc Donald. Nostro Signore degli Hamburger sta prendendo accordi con alcuni dei più noti fornitori di tecnologia wi-fi per dotarsi delle infrastrutture necessarie al collegamento wireless a banda larga. Così tra una patatina e l'altra i clienti potranno ingannare il tempo sfrecciando da un sito all'altro. E chissà mai che pur di navigare a velocità tanto golose, gli avventori siano disposti a ingollarsi molti più panini annegati nel ketchup di quanto fame o istinto di autoconservazione non suggeriscano.



NON SIAMO CATTIVI, SIAMO SOLO CURIOSI.



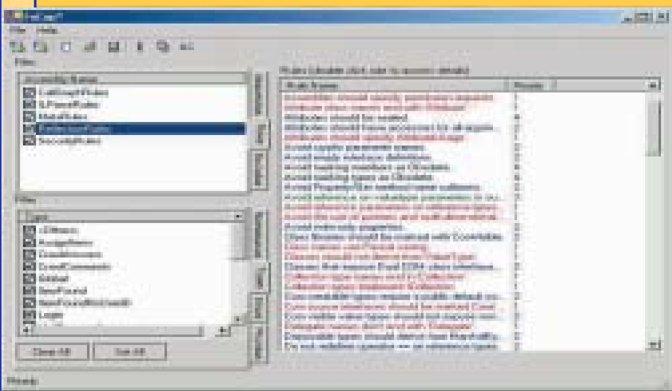
Hacker e Cracker. Due sole lettere di differenza per indicare categorie di persone tra cui c'è un abisso. Da una parte coloro che sono appassionati di tecnologie informatiche e che cercano di carpirne tutti i segreti possibili e immaginabili, restando nel lecito. Dall'altra persone a cui non basta il piacere della conoscenza, ma per sentirsi soddisfatti devono combinare malefatte informatiche a danno di terzi. Da una parte gli hacker dall'altra i cracker. Da una parte i buoni dall'altra i cattivi. Ci tengono a marcare questa netta divisione gli hacker, che per difendere la propria cultura e dignità di categoria, hanno anche fondato il progetto HANC. Acronimo di Hackers Are Not Crackers, o Hackers Are Not Criminals se preferiamo, questo manifesto sottolinea che gli hacker che non sono affatto pirati informatici come invece il dipingono i media, probabilmente per superficialità e ignoranza in materia. Chi volesse dare un'occhiata e dare il proprio contributo a diffondere la cultura hacker si può collegare al sito http://www.hancproject.org/.

PALMA D'ORO A NAPOLI



Si dice che San Gennaro protegga sempre i napoletani. Ma ci sa che questa volta il Santo nulla abbia potuto, per togliere alcuni suoi cittadini dalle grinfie delle forze dell'ordine. Tanto meglio, perché si trattava di persone disoneste che frodavano la legge sul diritto d'autore duplicando CD audio e software da rivendere sul mercato nero. Il bliz che la Guardia di Finanza ha portato a termine a Napoli negli scorsi giorni non ha precedenti. Sono stati individuati e messi sotto sequestro diversi laboratori altamente tecnologici con una capacità di duplicazione di circa tremila copie illegali all'ora. Nove le persone arrestate e trecentomila euro il valore della merce ritirata. All'operazione spetta la palma d'oro del più imponente sequestro mondiale di attrezzatura in termini di qualità e valore. Che dire, Napule è sempre Napule. Esagerata e grandiosa, nel bene e nel male.

L'UNIONE FA LA FORZA, SPERIAMO



Intorno a Bill Gates soffiano forti venti di apertura. Microsoft ha infatti annunciato di voler condividere con gli sviluppatori strumenti interni utilizzati per creare prodotti più sicuri e affidabili. Certo dato il numero di bug che esce dagli edifici di Redmond, c'è quasi da augurarsi che la condivisione di know how non superi certi limiti. Ma non vorremmo essere troppo cattivi. Vogliamo invece sperare che la collaborazione tra le persone possa dare i suoi buoni frutti come sempre. Tra le utility rilasciate ci sono Prefix e Prefast, due tool diagnostici che analizzano il codice sorgente in formato testo per trovare bachi nel codice C++. C'è un utilissimo programma che mette a disposizione degli sviluppatori uno schema su errori e vulnerabilità cui sono soggette le applicazioni già al momento della progettazione. Infine c'è FxCop un tool direttamente scaricabile all'indirizzo http://www.gotdotnet.com/team/fxcop/ che permette di evidenziare eventuali falle nella programmazione e controlla che il codice sviluppato sul modello MS.NET sia conforme alle linee guida del MS.NET Framework.

L'ULTIMA MAGIA DI HARRY POTTER



Nel carnet delle possibili magie del simpatico maghetto occhialuto ci deve essere anche quella di far sparire i siti. Se no non si spiega come mai sia stato parzialmente oscurato il sito del radicale Pietrosanti, promotore di un'iniziativa che riguarda, guarda caso, proprio Harry Potter. Insieme a un gruppo di non vedenti Prietrosanti sta organizzando una prossima vendita online della versione digitale dell'ultimo episodio della saga di Harry Potter a soli 4,8 euro. Prezzo che andrebbe a coprire i soli costi dei diritti d'autore. Si capisce che la faccenda abbia scatenato le ire degli editori, (Salani), che hanno promesso guerra e vendetta per una simile onta. E soprattutto per le presunte perdite economiche che tale vendita online comporterebbe. Quello che non si capisce è perché oscurare il sito di Pietrosanti, visto che non contiene nessun tipo di materiale illegale. A meno che non si consideri illegale la promozione dell'iniziativa e le ragioni che la giustificano. Ancora di meno si capisce come mai da uno dei due siti di Pietrosanti, www. pietrosanti.org invece sia ancora possibile scaricare la versione elettronica di Delitto e Castigo di Dostoevskji. La risposta viene da sé, ed è di sette lettere: censura. La guerra tra le due parti si preannuncia aspra e cruenta. Salani giura di trascinare Pietrosanti in tribunale qualora la vendita online abbia inizio. Pietrosanti e discepoli promettono che il libro in versione digitale verrà comunque distribuito. Attendiamo ansiosi gli sviluppi della contesa.

CARTUCCE IN LIBERTÀ



Forse non tutti sanno che cosa ci stanno a fare i chip sulle cartucce delle stampanti. Per protezione. Trattandosi di dispositivi protetti dal copyright, i chip hanno come unico scopo di impedire la ricarica delle cartucce ed evitare che produttori non autorizzati ne realizzino di compatibili. O meglio, così credevano i big delle cartucce fino a poco tempo fa. Ora una sentenza negli Stati Uniti ha cambiato le carte in tavola. Nel 2002, sicura di vincere, Lexmark ha fatto causa alla società SCC per avere creato cartucce compatibili che riproducevano il funzionamento dei chip Lexmark. Invece il tribunale ha dato ragione alla SCC. C'è infatti una sezione del DMCA, Digital Millennium Copyright Act, che permette alle aziende di sviluppare software allo scopo di rigenerare cartucce di toner e stampanti. La SCC pertanto potrà tranquillamente vendere chips sostitutivi da usare con le vecchie cartucce Lexmark.

LINUX IN DIRITTURA D'ARRIVO



Linus Torvalds & C. l'hanno definita "una significativa pietra miliare". Sarà anche che ogni scarrafone è bello a mamma sua. Ma questa volta il giudizio è obiettivo. Pare che la versione 2.6 del kernel di Linux potrebbe essere la penultima prima della versione finale. Già qualche settimana fa Torvalds aveva assicurato che nelle release non ci sarebbero state altre modifiche che non riguardassero strettamente la correzione di problemi di stabilità del kernel. Il consorzio in cui Torvalds e collaboratori ha esortato fornitori di sistemi, venditori indipendenti di software e clienti di Linux, a provare e verificare la nuova versione 2.6.0-test9 per prepararsi "alla prossima production release di Linux".

HOT!

CHI VA PIANO VA LONTANO?



Per alcune persone downloadare patch dal sito Microsoft è come controllare la posta elettronica. Si va sul server quando capita durante il giorno e si checka. Qualcosa da scaricare c'è sempre. Adesso però Microsoft cambia musica. Gli aggiornamenti arrivano solo una volta al mese. Per dare il tempo agli sviluppatori di risolvere il problema come si deve e non fare brutte figure, come è successo in passato. E se c'è in giro un bug, calma e gesso. Peggio per chi se lo deve pappare. Non si morirà mica ad aspettare una trentina di giorni, no? Il concetto presto e bene, pare che a Redmond non sia ancora giunto. Qualcuno glie lo vuole spiegare?

PILOTI SIMULATI A MILANO

Il 22 e il 23 Novembre, presso il Parco Esposizioni di Novegro, a due passi dall'aereoporto di Milano Linate, si terrà il "Milano Flight Simulator Show 2003", una manifestazione tutta dedicata al volo simulato. Oltre agli stand degli espositori (produttori e distributori di hardware e software attinente al tema), e delle varie associazioni di utenti e giocatori, ci sarà uno spazio dedicato a convegni, seminari e presentazioni di sessioni di volo. Se siete appassionati di volo simulato, buttatevi in picchiata su Novegro (tra l'altro, se il vostro simulatore di volo ha una mappa dell'aereoporto di Linate, potete farci anche una ricognizione simulata prima della visita vera e propria).
Per info: http://www.takeoffonline.it



E c'è chi con

Attenzione! Lo chiamano Ethical Hacking, ma non c'entra nulla con l'etica hacker!

Dopo l'associazione hacker-criminale, insieme all'associazione cracker-criminale-pirata informatico sembra che si stia diffondendo quella di **hacker-esperto in sicurezza**. Tale associazione ha portato all'affermazione di una nuova **elite di specialisti che si definiscono ethical hacker** ed ha creato, o meglio, istituzionalizzato una nuova forma di hacking, nota appunto come ethical hacking, che consiste più o meno nel **farsi pagare per fare quello per cui gli hacker e i cracker sono arrestati o condannati**: penetrare nei sistemi informatici e aggirarne le protezioni. Non ha però nulla ha a che fare con l'"etica hacker" dei programmatori del MIT, e tanto meno con l'"etica hacker del lavoro" che, come spiega molto chiaramente Pekka Himanen, è qualcosa che **va ben al di là del "mi porto a casa la pagnotta programmando"**. Vediamo di che si tratta.



>> C'è anche l'hackeretico

Un articolo di Affari&Finanza del 3 febbraio 2003, dal titolo "C'è anche l'hackeretico...", spiega: "Rappresentano la filosofia "buona" della cosiddetta pirateria informatica. Sono al servizio delle aziende e testano la sicurezza dei computer". "L'approccio e l'insuperabile conoscenza dei sistemi informatici sono gli stessi degli hacker tradizionali: **adesso si guarda però al business** della gestione delle reti e della tutela della privacy. L'hacker etico o hacker eretico o hacker convertito, "in giacca e cravatta (sia pure metaforicamente)", o in qualunque modo lo si voglia definire, rimane però ancora fedele, così si dice, alla filosofia e allo spiri-

NEWBIE

L'HACKING si è fatto i soldi...

to del vero hacker. Tra coloro che praticano questa nuova forma di hacking si menzionano **Secure Group**, **Gecko Network** insieme ai **Black Hats**. Questi ultimi sono i primi ad aver parlato di ethical hacking, ma in maniera molto diversa dagli altri. Li considereremo quindi come un caso a parte.

Come gli hacker, gli specialisti di Secure Group e di Gecko Network, sfruttano dei bug dei sistemi per lanciare degli attacchi, sia dall'esterno tramite la rete internet sia dall'interno. Ma sottolineano: **"non intendono né danneggiare i sistemi né sottrarre informazioni riservate"**. Si tratta infatti di semplici simulazioni: viene riprodotto "il modus operandi di un hacker/cracker" e "l'attacco effettuato da persone con un accesso o una conoscenza delle risorse interne dell'azienda". In questo modo si può valutare la sicurezza dei sistemi, redigere dei report da consegnare ai proprietari in cui vengono descritte le vulnerabilità e intervenire per difendere adeguatamente il sistema. Non si limitano a identificare i problemi, **"ma aiutia-**

Raoul Chiesa



Dei Black Hats ha fatto parte anche Raoul Chiesa aka Nobody, un hacker o ex hacker che oggi pratica quello che egli definisce l'"hacking del lavoro": si occupa di sicurezza informatica, protegge i sistemi e crea prodotti I.T. Security. "Hacking, nel senso più puro del termine", spiega Chiesa, "significa ricercare i difetti, gli errori. Scoprirli, renderli noti, risolverli. La Security, nel significato più pratico del termine, significa fare attenzione ai difetti ed agli errori. Scoprirli, renderli noti, risolverli. Hacker e Security Researcher vivono dunque tra bug, exploits, security advisory, testing, reverse engineering". Chiesa è convinto che la sicurezza non possa fare a meno della ricerca e della sperimentazione underground e che l'unico modo per saggiarne la robustezza sia provare a forzare i sistemi. Parla dell'hacker come di un "amico della sicurezza" e descrive l'ethical hacker come: "colui che hackera il vostro sistema, lo esplora velocemente e ve lo fa persino sapere, inviandovi mail di report o suggerimenti". E' quello che fa anche Chiesa, ma per lavoro. Tra i servizi offerti dalla sua azienda (Mediaservice) vi è il Security Probe, o Penetration Test: "il cliente ci richiede di violare, con tutti gli strumenti possibili, la propria rete aziendale, sfruttando tutte quelle dimenticanze, errate configurazioni o bug lasciate dai fornitori abituali". A chi lo accusa di essere passato dall'altra parte, spiega: "Quando mi sono avvicinato all'hacking per la prima volta vedevo questo mondo come un luogo sacro, una religione, uno stile di vita, un modo di pensare e agire. La penso ancora così. Ho rifiutato spesso di procedere o partecipare all'identificazione di hacker responsabili di violazioni di sistemi, ma non di danni. Perchè hacking, per me, continua a voler dire libertà, sfida, essere più bravi...Non credo di condividere le idee comuni dei responsabili o esperti di sicurezza informatica. Continuo a sentirmi hacker". Chiesa è un hacker ma non è la sua attuale professione ad averlo reso tale. Lo status e la fama di hacker, già "vasta nella cominità hacker europea", gli è stata "riconosciuta e suggellata" dalle autorità internazionali "dopo una serie di eclatanti intrusioni in grossi Enti e Istituzioni - tra le quali Bankitalia, IBM e AT&T".



mo anche a definire soluzioni su misura degli obiettivi di business", sostiene Gecko Network. Sempre come un hacker, lo specialista Secure Group, svolge la sua attività con creatività e il suo scopo è innanzitutto sfidarsi e superare se stesso. Il vero spirito hacker è messo al servizio della sicurezza dei sistemi. Anche lo specialista di Gecko Network si preoccupa della sicurezza informatica delle aziende e il suo scopo è quello di salvaguardare "le molte cose buone che ha portato la crescita esplosiva di Internet", tra cui il commercio elettronico, un accesso facile a una quantità immensa di informazioni, il collaborative computing, l'e-mail, nuove strade per la pubblicità e la distribuzione di informazioni. Da notare come la distribuzione di informazioni venga menzionata accanto alla pubblicità, considerata altrettanto positiva!! (?) Secure Group usa il termine **"ethical"** perché "vuole dare a questa forma di intrusione autorizzata dei sistemi, l'aggettivo morale (lecito), a pro di una giusta causa: migliorare le difese del sistema informativo aziendale". Benché lo spirito d'intraprendenza sia quello di un hacker, Secure Group ribadisce che l'attività di "hacking etico" è a fini costruttivi e **"in totale contrasto con l'attacco di un cracker mirato alla distruzione di un obiettivo o comunque alla sua compromissione per secondi fini"**. Anche Gecko Network fornisce una descrizione dell'ethical hacking, ma nell'area "prodotti": "I governi, le aziende, i privati cittadini di tutto il mondo sono ansiosi di essere parte di questa rivoluzione, ma temono che qualche hacker entri nei propri web server e rimpiazzi il logo aziendale con immagini pornografiche, che possa leggere le e-mail, che possa intercettare il numero di carta di credito da un sito di shopping on-line, o installare qualche software che rende pubblici i segreti della propria azienda. Con queste ed altre preoccupazioni, l'hacker etico può essere d'aiuto". Ma **nel frattempo, il vero hacker si è parecchio incavolato nel vedersi associato persino alla pornografia!**



>> Black Hats e Raoul Chiesa

I Black Hats sono stati promotori dell'ethical hacking, ma **hanno chiuso i battenti il 6 marzo 2003**, perchè lo scopo che si erano proposti era ormai stato raggiunto: **"portare alla luce le conoscenze nascoste nell'underground tecnico italiano"**. Però chiariscono: si è conclusa solo questa esperienza, non il loro compito, ed è per questo che ne parleremo al presente. I Black Hats **mettono le proprie capacità a disposizione del prossimo** per rendere più sicura la digital life. Formano un'**associazione senza scopo di lucro**, non legano il loro nome a prodotti commerciali di alcun genere, in quanto vedono nella "filosofia Vendor Independent **l'unico modo per assicurare l'imparzialità e l'oggettività** nel campo dell'ICT Security". Molti di loro lavorano nel campo della sicurezza informatica per altre aziende, ma quella dei Balck Hats non è un'attività lavorativa, non ci guadagnano nulla e non effettuano penetration test, security assessment o product testing. La loro funzione primaria è quella di **divulgare la cultura nel campo della sicurezza**, attraverso speech tecnici e attività di ricerca, diffondere informazione

seria, corretta e veritiera sull'hacking che essi considerano "a state of mind", uno stile di ricerca e di vita, "affinchè i mass-media non commettano più i tipici errori nel comunicare informazioni sull'hacking, ricadendo in luoghi comuni con termini diffamatori e falsi come "pericolose bande di hacker" o "anarco-hacker" o "tecnobanditi" o ancora "pirati informatici" e "terroristi del web". I Black Hats cercano di fare cultura, così affermano, non solo sul piano tecnico ma anche filosofico/storico.

>> Pubblicità e falsa Informazione

Il termine "hacker", si legge nel **Jargon File**, tende a connotare l'appartenenza ad una comunità globale. Implica anche che la persona in questione sottoscriva in qualche modo l'etica hacker. Per un hacker etico è una forma di cortesia spiegare al sysop, tramite e-mail o da un account di superuser, esattamente come si è fatto ad entrare nel sistema e come il buco possa essere tappato. Questo hacker si comporta come un **"tiger team"** che nel gergo dell'esercito USA sta appunto per un esperto che segnala delle falle nei sistemi (non informatici) di sicurezza, lasciando, per esempio, in una cassaforte che si pensa sia custodita e in realtà non lo è, un cartellino che dice "avremmo potuto rubare i vostri codici". Solo che **l'hacker etico non è pagato e il suo intervento non è neanche richiesto**. Secure Group e Gecko Network, invece, propongono l'hacker come **"una nuova figura professionale del complesso mondo della New Economy"**. I loro specialisti sono nuovi hacker o ex-hacker che, a differenza di molti altri che **vendono le proprie conoscenze alle multinazionali**, fanno spionaggio elettronico o lavorano per i governi, hanno deciso di mettersi in proprio e al servizio delle aziende e del business. **Ma non è questo che li rende etici!** Lo diventano nel momento in cui confrontano il fine della loro attività - ma **non lo spirito e neanche la tecnica** -, con quello degli hacker e dei cracker cosiddetti "criminali" o "pirati". L'Ethical Hacking, proposto da queste aziende, non è una filosofia e in realtà non è neanche un'etica. Viene, infatti, da essi stessi definito **una metodologia, un servizio, un prodotto**. Gecko Network offre quattro tipi di test di ethical hacking; Secure Group fornisce moltissimi servizi di ethical hacking.

Gli ethical hacker di Gecko Network e Secure Group salvaguardano la sicurezza dei sistemi informatici, **tutti gli altri hacker danneggiano, rubano informazioni riservate o entrano nei sistemi per secondi fini illeciti**. Un vero hacker o chi ha capito come la pensano, **non incorrerebbe in questo errore**, già abbondantemente perpetrato dai media. Nonostante l'opera di diffusione di una cultura dell'hacking anche da parte dei Black Hats, i primi a definirsi ethical hacker, c'è ancora chi, sventolando la bandiera di "una strana e non ben definita etica hacker", associa gli hacker a immagini pornografiche e i cracker e persino gli hacker a coloro che entrano nei sistemi informatici per far danno. Per un hacker etico l'informazione è tutto, soprattutto se "veritiera"! Ma questa non lo è! La diffusione della cultura informatica ha sicuramente aperto la strada a nuove forme di criminalità. Questa criminalità, però, è sempre solo e unicamente associata agli hacker, **persino dagli ethical hacker**. Gecko annovera "le molte strade della pubblicità" tra le molte cose buone che ci ha dato internet. Descrive l'hacker come colui che installa "qualche software che rende pubblici i segreti della propria azienda". La pubblicità però è una delle tante forme di intrusione non autorizzata, forse la più diffusa. Accade spesso che software cosiddetti legali contengano al loro interno degli **"Spyware"**, programmi che comunicano informazioni sul nostro conto. Queste informazioni vengono poi usate, senza che nessuno ce l'abbia chiesto, per fini statistici, ma più spesso per inviarci pubblicità indesiderata, il cosiddetto **"Spam"**. **Nessuno parla di queste intrusioni come di crimine o pirateria!** L'ethical hacking è a nostro parere un fenomeno che **trae i suoi frutti e i suoi vantaggi proprio dalla criminalizzazione degli hacker e dei cracker**. Più i media parlano di hacker e cracker criminali informatici, più questa nuova forma di hacking si alimenta e trae i suoi proffitti. Come rileva Raoul Chiesa in un suo articolo dal titolo "Il difficile rapporto tra hacking e marketing" **l'associazione hacker-pubblicità** sta andando molto di moda. Si amplifica la portata degli attacchi hacker per invocare stati d'assedio fittizi. Si vende un servizio perché si genera paura e contro la paura alcune aziende hanno il rimedio. Nella strategia militare, simili tecniche, affatto corrette, si raggruppano sotto il nome di Propaganda e disinformazione.

DaMe`
www.dvara.net/HK

BIBLIOGRAFIA E SITOGRAFIA

Italian Black Hats:
http://www.blackhats.it

Gecko Network:
http://www.geckos.it

Secure Group:
www.securegroup.it

Affari&Finanza - Susanna Jacona Salaria: C'è anche l'hackeretico…:
http://www.securegroup.it/rs/feb_03_affariefinanza.pdf

Raoul Chiesa: Il difficile rapporto tra hacking e marketing:
http://www.internos.info/archivio/rc16.pdf

Biografia e molti articoli di Raoul Chiesa:
http://www.lamerone.net/raoul/00_whois.php



PESCARE NELLA MEMORIA

Sveliamo le informazioni che vagano nella memoria durante il funzionamento dei programmi.

Non fraintendete il titolo, non vi servono canna, lenza ed amo! Basta un buon debugger ed un po' di ingegno! Niente grigliata di trote, ma un altro programma da analizzare. Quella che dobbiamo trovare è la soluzione di **un altro gioco scritto e pensato per gli aspiranti reverser che leggono la rivista**. L'analogia con la pesca tradizionale può sembrare una mia eccentrica trovata, ma in realtà quella che useremo è una **tecnica ampiamente diffusa** tra i reverser di tutto il mondo e conosciuta proprio con il nome di **"fishing"**, che significa "pescare".

>> Il programma da studiare

Dimenticatevi il programmino minuscolo che abbiamo smontato assieme nel numero 36. Ora abbiamo per le mani **qualcosa di un po' più complesso**. C'è un'interfaccia grafica, un'immagine, un riquadro contenente una domanda, una casellina in cui immettere la risposta ed un tasto da premere. Il funzionamento è abbastanza intuitivo, ci sono tre quesiti a cui rispondere in sequenza, tutto qui. I primi due quiz sono volutamente semplici mentre per il terzo dovete ricorrere al reversing. Per rendere ancora più sfiziosa la sfida, **non troverete i sorgenti** del programma insieme all'eseguibile, né conoscerete la soluzione completa leggendo questo articolo fino in fondo. Pensate sia meschino? Tutt'altro! Lo sarei se vi dessi tutte le risposte, togliendovi il gusto di risolvere da soli l'enigma, un po' come quei simpaticoni che ci raccontano il finale dei film che non abbiamo ancora visto! Per quanto concerne i sorgenti, poi, vorrei ricordarvi che il **reverse engineering** viene praticato proprio quando i listati dei programmi **non sono disponibili**. Tanto per alzare la posta in gioco, invierò il codice sorgente del giochino, scritto in **Macro Assembler**, a tutti coloro che mi daranno la risposta corretta alla terza domanda attraverso la posta elettronica.

>> Debugging con OllyDbg

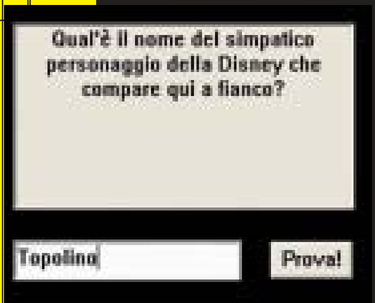
Siccome molte persone mi hanno segnalato difficoltà di reperimento e di installazione di **SoftICE**, ho pensato di utilizzare un debugger diverso per questo articolo. **OllyDbg**, a differenza di SoftICE, **non deve essere installato come un driver di sistema,** ma si può utilizzare come un normale programma. Questa caratteristica lo rende estremamente semplice da installare e poco invasivo per il nostro computer. Si perde la possibilità di sbirciare nel nucleo più interno e nascosto del sistema operativo e non si possono studiare i drivers, ma per analizzare i comuni programmi è più che sufficiente. C'è da dire, poi, che è completamente gratuito per uso privato! Facciamo partire, quindi OllyDbg e apriamo il file **giochino2.exe** (si trova nella Secret Zone di hackerjournal.it) utilizzando i classici menu o, più semplicemente, trascinandone l'icona sulla finestra del debugger. Ciò che appare ai no-



stri occhi è una schermata piuttosto densa di informazioni e divisa in quattro parti. Nel riquadro in alto a sinistra, il più interessante per noi, appare il **disassemblato** del programma e subito sotto c'è il **dump del suo segmento dati**. Nella parte destra, invece, in alto compaiono i registri della **CPU** ed in basso il dump dell'area **stack**. Concentriamoci sul riquadro contenente il codice del programma e notiamo come tutte le funzioni esterne vengano colorate in rosso.

>> Analizziamo il nuovo giochino

Possiamo scorrere il disassemblato con i tasti **PageUp** e **PageDown** o utilizzando la barra di scorrimento laterale, ma cerchiamo di non farci spaventare dalla quantità di istruzioni assembly e dal numero di routine chiamate. Tutto sommato, a noi interessa solo una funzione, cioè quella con cui il programma legge la risposta che abbiamo scritto nella casellina in basso. Questa funzione è **GetWindowTextA()**, quindi cerchiamola (si trova all'indirizzo **4012C5**), selezioniamo la riga cliccandoci sopra e premiamo **F2** per fissare un **breakpoint**! Per chi vuole usare SoftICE, il comando analogo **bpx GetWindowTextA**. A questo punto premiamo sul tasto a forma di **triangolino verde** (come il "play" dello stereo) di OllyDbg, o, se usiamo SoftICE, facciamo semplicemente partire il programma. Il giochino appare sullo schermo e ci chiede di indovinare il nome di un simpatico personaggio della Disney rappresentato in un'immagine. Ovviamente si tratta di Pippo, ma supponiamo di non saperlo e nel riquadro scriviamo **"Topolino"** premendo, subito dopo, il tasto **"Prova!"**.



OllyDbg fa' il suo dovere e si blocca proprio dove avevamo settato il punto di arresto precedentemente. Andiamo avanti di qualche riga con il tasto **F8** per chi usa OllyDbg e **F10** per chi ha SoftICE fino ad arrivare all'istruzione **CMP EAX, DWORD PTR DS:[4033A1]**. Analizziamo ciò che è successo. Il programma legge la nostra risposta usando la funzione già citata e la memorizza all'indirizzo **4031A1**. Subito dopo la funzione **lstrlenA()** conta il numero di caratteri della parola che abbiamo fornito e mantiene tale valore nel registro **EAX**. A questo punto c'è l'istruzione **CMP** che confronta il valore di **EAX** (in questo caso 8) con quello memorizzato nel segmento dati del programma all'indirizzo **4033A1**, cioè 5. Se l'esito del confronto è negativo, viene visualizzata la finestrella che dice che abbiamo sbagliato, altrimenti si salta in avanti all'indirizzo **401301**. È evidente, quindi, che la nostra risposta deve essere di cinque lettere, ma possiamo comunque sbirciare all'indirizzo citato poc'anzi per vedere come continua l'esecuzione. Ci sono un paio di **CALL** a funzioni interne al programma e poi c'è una chiamata a **lstrcmpA()** che serve a confrontare due stringhe, dove la prima è il nome che abbiamo immesso noi, mentre la seconda è molto strana. Evidentemente la risposta esatta è stata criptata per rendere più difficile (in questo caso più divertente) il lavoro ai reverser. Premiamo **OK** sulla finestrella che compare dicendoci che abbiamo sbagliato e ritentiamo provando a rispondere con una parola di cinque lettere, ad esempio, **"Pluto"**.

>> Osservare il programma

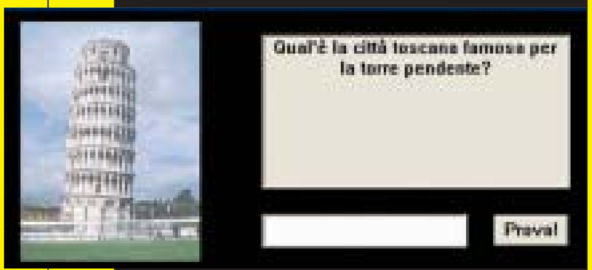
Premiamo ripetutamente **F8** per seguire passo passo l'esecuzione del programma senza però entrare nelle varie subroutines chiamate e vediamo cosa succede. L'istruzione di salto condizionato di prima questa volta viene eseguita e possiamo verificare l'effetto delle funzioni chiamate dalle due istruzioni **CALL** che avevamo notato poco fa. Non serve nemmeno entrare nelle funzioni stesse per capire che la prima converte tutte le lettere della nostra risposta in maiuscole, visto che la parola **"Pluto"** viene trasformata in **"PLUTO"** e che la seconda decripta la "strana parola" di prima e la trasforma in "PIPPO". A cosa servono queste due funzioni? La prima permette di accettare indifferentemente lettere maiuscole e



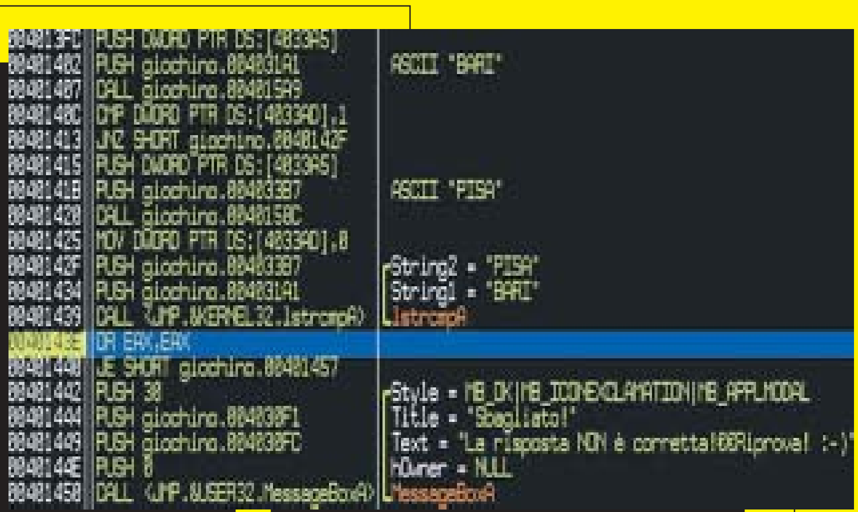
minuscole in modo che “Pippo” , “PIPPO” , “pippo” , “pIpPo” , ecc siano considerate tutte corrette, mentre la seconda serve ad impedire che il **lamer** di turno trovi le risposte corrette leggendole in chiaro all’interno del file exe senza nessuno sforzo di reversing. Bene, abbiamo capito che la risposta giusta è **“PIPPO”**, quindi riproviamo ancora rispondendo correttamente. Siccome sappiamo che questa volta la soluzione è esatta, la prima volta che OllyDbg intercetta la chiamata alla funzione **GetWindowTextA()** possiamo dire al nostro simpatico debugger di continuare a far correre il programma fino a che tale funzione non verrà chiamata per la seconda volta.

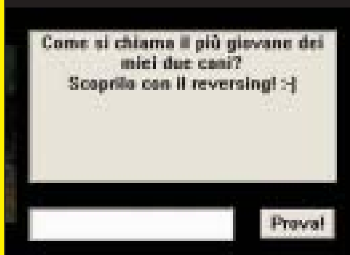
Seconda prova

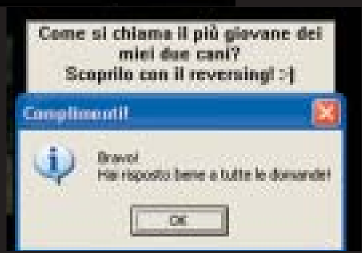
Compare la foto della torre di Pisa, ma noi, fingendoci più ignoranti di Homer Simpson, rispondiamo che la città in

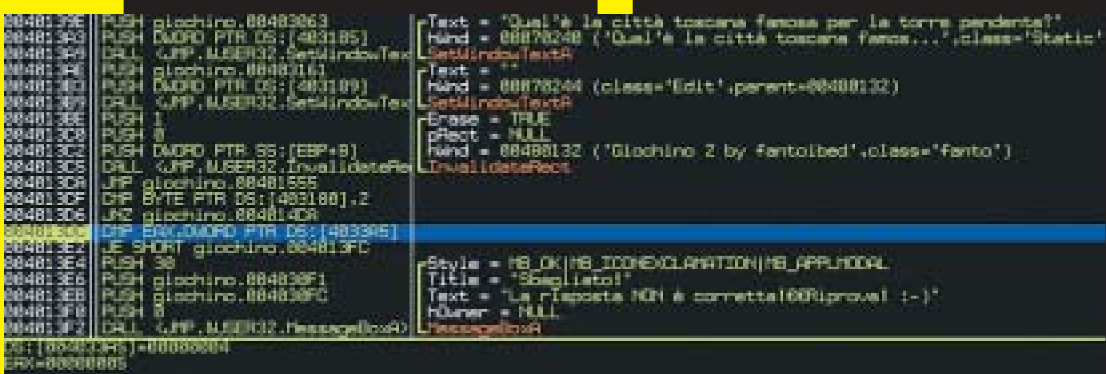


questione è **“Udine”**! Premiamo il tasto **“Prova!”** e ripercorriamo il cammino precedente. Notiamo subito che dopo la chiamata alla funzione **lstrlenA()** c’è un salto condizionato e che il confronto tra il registro **EAX** contenente la lunghezza della parola **“Udine”** da noi inserita e la lunghezza della risposta esatta viene eseguito dopo tale salto e, più precisamente, all’indirizzo **4013DC**, dove, appena giunti, possiamo notare che la parola corretta da inserire è di quattro lettere. Proviamo, quindi, a rispondere **“Bari”** e **“steppiamo”** con **F8** fino a che il programma non avrà decriptato la risposta esatta servendocela in un piatto d’argento. La terza domanda è l’unica di cui non potete conoscere la risposta a meno che non siate i miei vicini di casa, visto che si tratta di indovinare il nome di uno dei miei due cani. Il procedimento è del tutto analogo a quello seguito finora e, siccome non voglio toglervi il divertimento, lascio a voi l’onere e l’onore della sfida. Ricordatevi che









la funzione **lstrlenA()** restituisce la lunghezza di una stringa nel registro **EAX** e quindi dovete aspettarvi un confronto del tipo **CMP EAX, DWORD PTR [QUALCOSA]**, dove **“QUALCOSA”** è l’indirizzo di memoria che contiene la lunghezza della risposta corretta, dopodiché dovete immettere una parola della stessa lunghezza della soluzione reale e seguire l’esecuzione del programma fino a che non avviene il confronto tra la parola inserita da voi e la soluzione reale. Lasciamo quindi che sia il programma a decrittare per noi la risposta corretta e leggiamola come argomento di **lstrcmpA()**. Se usate SoftICE, vi ricordo che il contenuto dei buffer non viene visualizzato automaticamente, ma dovete usare il comando dump come abbiamo fatto per il primo giochino.

Conclusioni

Se avete capito il meccanismo, non vi sarà difficile scoprire il nome del mio cagnolino. Se me lo comunicate per email, come premio, posso inviarvi i sorgenti del programma che, come ho già detto, è in **Macro Assembler**. Se avete problemi o vi piantate in qualche passaggio, interpellatemi pure attraverso la posta elettronica e, compatibilmente con la mia disponibilità di tempo, provvederò a dissipare i vostri dubbi. Buon divertimento!

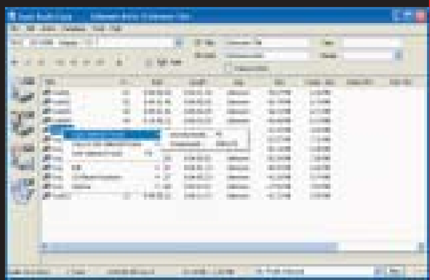
fantoibed
fantoibed@libero.it

TUTTA UN'ALTRA MUSICA!

Sei programmi gratuiti per rippare, codificare, ascoltare, visualizzare, ordinare, ripulire, approfondire, analizzare la vostra collezione di file musicali.

Exact Audio C

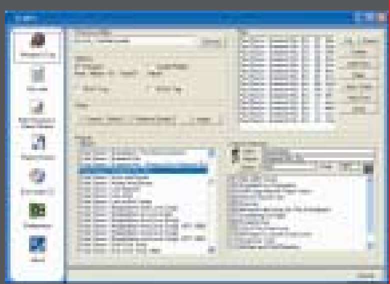
www.exactaudiocopy.de



Come il nome lascia intendere, Exact Audio Copy è un programma per estrarre le tracce audio da un CD, ed è un compito che svolge molto bene. È in grado di lavorare sia con CD Scsi che ATAPI, e ha tre diversi livelli di estrazione: Sicura, Veloce e "Lampo". Nella modalità Sicura è in grado di applicare sofisticati algoritmi per la correzione degli errori (quei rapidissimi "bip" che ogni tanto si sentono negli MP3 estratti in modo grossolano…). Recupera le info sui nomi delle tracce da un database locale o da CDDB.com, e supporta persino alcuni masterizzatori per registrare CD senza bisogno di usare altri programmi. Come "pagamento", l'autore chiede che gli si spedisca una cartolina. Per le qualità del software, ne merita almeno dieci.

K-MP3

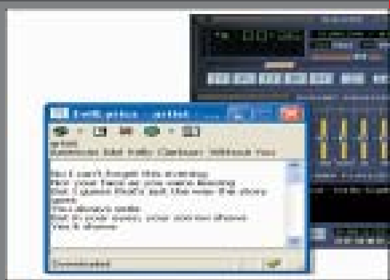
www.katarncorp.com/?kmp3



Anche voi odiate il disordine? K-MP3 può darvi una mano, per lo meno per quanto riguarda la collezione di file audio. È infatti utilissimo per aggiungere o modificare e i nomi dei file MP3, prelevandoli dal servizio online FreeDB, e ripulirli in vario modo (convertire gli spazi in trattini, cambiare le maiuscole in minuscole), e permette di creare playlist personalizzate. Supporta i formati mp3, ogg, vqf, wma, wav, mpc e ape.

EvilLyrics

www.evillabs.sk



EvilLyrics lavora in accoppiata con WinAmp o altri riproduttori di Mp3 e si occupa di recuperare da Internet il testo della canzone attualmente in riproduzione, e di visualizzarlo in una piccola finestra. Altre opzioni permettono di effettuare ricerche su Google, Amazon e vari strumenti di traduzione per ottenere tutte le informazioni possibili sull'autore e sul brano che si sta ascoltando.

Fmod

www.fmod.org



A qualcuno piace semplice. Altri preferiscono potenza, versatilità e un'interfaccia magari complicata, ma completissima. Inutile negarlo: Fmod è indicato per il secondo tipo di persone. Permette di riprodurre file mp3, ogg vorbis, wma, midi, mod, streaming da Internet. Il tutto visualizzando lo spettro audio e applicando effetti audio anche 3D. Nonostante le funzionalità, consuma pochissime risorse del processore.

MilkDrop

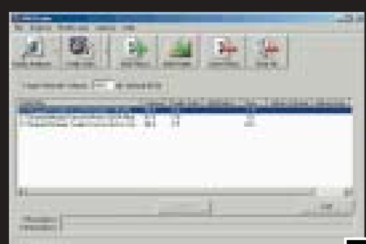
www.nullsoft.com/free/milkdrop/



MilkDrop è un semplice plug-in di visulizzazione per WinAmp. Prima di catalogarlo tra la "fuffa", leggete un po' cosa è capace di fare. Innanzi tutto, oltre a funzionare sia in una finestra che a tutto schermo, può anche sostituirsi allo sfondo Scrivania; potete quindi continuare a lavorare normalmente, ma con lo sfondo in continuo movimento e a tempo di musica. Inoltre, potete inserire una qualsiasi equazione matematica, che MilkDrop userà come base per la visualizzazione di effetti sempre nuovi. Un must, che però richiede una scheda con accelerazione 3D hardware e il supporto di DirectX.

MP3Gain

http://mp3gain.sourceforge.net



Vi capita mai di stare per addormentarvi ascoltando l'Adagio di Albinoni, suonato piano, per poi svegliarvi improvvisamente con l'ultimo dei System Of A Down sparato a massimo volume? MP3 Gain evita questo e altri problemi, analizzando e "livellando" il livello di uscita della vostra collezione di Mp3, in modo da non avere grossi sbalzi tra un brano e l'altro. Purtroppo, non può fare nulla per rendere un po' più umani i vostri accostamenti musicali.

Bios: nel

Cosa succede esattamente quando premiamo

Come avviene il passaggio dalla pressione del tasto di accensione alla visualizzazione del nostro desktop pieno di icone (Windows o Linux che sia)? Proviamo ad immergerci nelle viscere del nostro PC, e a scoprirne i meccanismi più interni, spingendoci laddove i normali uomini si fermano, ma gli hacker sono di casa.

>> L'avviamento

Il semplice gesto di premere il pulsante di accensione del PC dà il via a una complessa procedura di avviamento, suddivisa in varie fasi:

1) Avvio BIOS
2) P.O.S.T: (Power On Self Test, ossia auto-test di accensione)
3) Lettura MBR (Master Boot Record) del disco di avvio
4) Avvio del Loader dell'MBR

A questo punto si ha una differenziazione tra sistemi basati su Linux, DOS/Windows o NT:

LINUX:
5) Avvio di LILO (Linux Loader)
6) Caricamento Kernel
7) Montaggio ROOT
8) Avvio di INIT (processo padre di tutti i processi)
9) Lettura /etc/inittab
10) Ecc. ecc

DOS:
5) Esecuzione IO.SYS
6) Esecuzione MSDOS.SYS
7) Esecuzione CONFIG.SYS
8) Avvio shell impostata sul CONFIG.SYS, oppure avvio COMMAND.COM
9) Avvio AUTOEXEC.BAT, oppure settaggio data e ora (se AUTOEXEC.BAT assente)
10) Prompt dei comandi

Windows 95/98/ME: (= ambiente DOS con interfaccia grafica Windows)
5) Esecuzione IO.SYS
6) Lettura MSDOS.SYS (file di testo con parametri di configurazione)
7) Esecuzione CONFIG.SYS
8) Avvio shell impostata sul CONFIG.SYS, oppure avvio COMMAND.COM
9) Avvio AUTOEXEC.BAT, oppure settaggio data e ora (se AUTOEXEC.BAT assente)
10) Avvio dell'interfaccia grafica Windows.

Windows NT/2000/XP: (= sistema operativo grafico, non basato su DOS)
5) Esecuzione NTLDR - passaggio a modalità protetta con indirizzamento a 32 bit (non effettuato in DOS)
6) Esecuzione NTDETECT.COM - rilevamento configurazione hardware
7) Lettura file BOOT.INI, presentazione menu per scegliere quale Sistema Operativo avviare (se più di uno presente sull'hard disk)
8) Se viene scelto un S.O. diverso da NT, il controllo bassa a BOOTSECT.DOS
9) Se viene scelto NT, il controllo passa a NTOSKRNL.EXE (nella cartella SYSTEM32).

Vediamo prima la parte comune:

>> Avvio Bios

Alla pressione del tasto di accensione, si accende **l'alimentatore** del PC, che dopo poche frazioni di secondo è in grado di erogare la corrente necessaria al funzionamento del PC: quando ciò accade, l'alimentatore invia un opportuno segnale (**PowerGood**) alla CPU, che inizia a eseguire il suo primo programma. Poiché il computer è stato appena acceso, non potrà esserci **nessun programma in memoria RAM**, per cui la CPU cercherà qualcosa da eseguire in ROM: **il BIOS, appunto**. A che indirizzo di memoria si trova la ROM del BIOS? La CPU è programmata in fabbrica per eseguire, appena accesa, il codice contenuto a partire dalla locazione **ffff0**; siccome l'ultima locazione del primo megabyte (quello accessibile al PC appena acceso) è **fffff**, il codice potrà essere lungo al mas-



cuore del PC

il tasto di accensione del nostro PC?

Il BIOS

B.I.O.S sta per Basic Input Output System, ovvero "sistema di base di ingresso/uscita": il BIOS è infatti un circuito che collega fisicamente il cuore del PC, ossia la CPU (Central Processing Unit, unità centrale di elaborazione) ai vari componenti (l'hardware) del PC (hard disk, tastiera, scheda video, scheda audio, memoria ecc…), fungendo così da interfaccia.

Il modello del BIOS è identificato da una stringa di caratteri che compare sullo schermo all'avvio del PC, nella forma xx-xxxx-xxxxxx-xxxxxxxx-xxxxxx-xxxxxxxx-x (ogni "x" è un numero); potete decodificare questa stringa andando a questa pagina: http://burks.bton.ac.uk/burks/pcinfo/hardware/bios_sg/bios_sg.htm



Il Master Boot Record

Offset	Dimensione	Contenuto
+0	1Beh (446 decimale)	Partition Loader Code
+1BEh	10h (16 decimale)	Informazioni partizione 1
+1CEh	10h (16 decimale)	Informazioni partizione 2
+1DEh	10h (16 decimale)	Informazioni partizione 3
+1EEh	10h (16 decimale)	Informazioni partizione 4
+1FEh	2 (2 decimale)	55 AA (Identificativo tavola partizioni: 0AA55h)
tot	1ffh (512 decimale)	

Alcuni documenti interessanti sulla gestione dell'MBR si trovano agli indirizzi:
http://thestarman.narod.ru/asm/mbr/BootToolsRefs.htm,
http://home.att.net/~rayknights/pc_boot/debug.htm#GetMBR2

simo **16 bytes** (da ffff0 a fffff, appunto). In realtà, il codice effettivo è ancora più corto: c'è una semplice istruzione di **JUMP** (codice assembly: **EA**) seguita da un indirizzo a 20 bit (quindi 4 bytes), per un totale di **5 bytes**; i restanti 11 contengono **la data di creazione del BIOS** in formato testo (mm-gg-aaaa) e un byte che identifica se il BIOS è di tipo **XT** (vecchissimi computer, con processore 8088) o **AT** (computer moderni): trovate una tabella a questo indirizzo, anche se probabilmente non comprende tutti i valori possibili: www.powernet.co.za/info/BIOS/sys_id.htm.
L'utilizzo dell'ultimo byte sembra sia sconosciuto… (www.cybertrails.com/~fys/rombios.htm).
L'istruzione di **JUMP** salta alla posizione effettiva del codice del BIOS.
Il programma contenuto nella ROM del BIOS esegue compiti molto elementari:

***primo Power On Self Test (P.O.S.T)**:controllo integrità dell'hardware; in caso di errore in questa fase, non essendo ancora stata inizializzata la scheda video, il BIOS comunicherà gli errori all'utente mediante codici sonori, che differiscono da produttore a produttore; all'indirizzo www.pcguide.com/ts/x/sys/beep trovate una spiegazione del loro significato, divisa per marca di BIOS (AMI, AWAWRD, PHOENIX o altri).
***ricerca di BIOS di altro hardware** (in genere è la scheda video ad aver un suo BIOS; per questo motivo, su alcuni computer, il logo della scheda grafica compare sul monitor prima di qualunque altra informazione.
***controllo se l'avvio è stato "a freddo"** ("cold boot", accensione del PC) **o "a caldo"** ("warm boot", reset del PC): se la locazione 0000.0472 contiene il valore 0x1234, è un "warm boot".

>> P.O.S.T. (secondo)

Le informazioni relative a questo POST, a differenza del precedente, sono **visualizzate sul monitor**, essendo già stata inizializzata la scheda video. Sarà quindi possibile vedere il progresso nel controllo della memoria, i dati relativi al sistema (**temperatura** CPU, **voltaggi** di sistema eccetera). Al termine del POST, se tutto è andato a buon fine il PC emetterà il classico **BEEP** tipico di ogni avvio.
A questo punto, il BIOS va a leggere le impostazioni memorizzate nella memoria CMOS.

>> Lettura MBR

M.B.R. sta per **Master Boot Record**, ovvero "record di avvio principale": è un'area del disco di avvio (che può essere l'hard disk, un floppy o, nei computer più recenti, un CD-ROM) che contiene i dati di base per l'avvio del PC. Esso è contenuto nel **Boot Sector**, il "Settore di avvio" del computer, ovvero il **primo settore del disco**, identificato dalle "coordinate" **Cylinder 0, Head 0, Sector 1** (vedi riquadro sulla descrizione della struttura di un disco)..
L'MBR è lungo **512 byte**, ed è composto di due parti: la **Partition Table** (tabella delle partizioni), e il **Partition Loader Code** (Codice di caricamento della partizione).
La tabella delle partizioni occupa solo **16x4=64 bytes**, mentre la maggior parte dello spazio (i 446 byte rimanenti, oltre i 2 di controllo finali) è occupata dal **Loader**. Se il nostro PC è dotato di un unico sistema operativo, il MBR provvederà ad avviarlo, mentre se ci sono più sistemi operativi, e quindi più partizioni, il MBR **avvierà un programma, detto bootloader** (contenuto nel Boot Sector dell'unica partizione di avvio del disco) che ci permetterà di scegliere quale sistema avviare.

L'avvio del Loader dell'MBR avviene con modalità diverse, a seconda del sistema operativo che si vuole lanciare.

Sistemi Linux:
il MBR conterrà un programma detto **LILO** (LInux LOader), che si occupa appunto di avviare Linux, seguendo la sequenza accennata sopra, descritta in dettaglio a questo indirizzo: www.ccoss.org/tutorials/lfs/Linux_from_Scratch_A_Tour.htm

Sistemi DOS:
Il loader dell'MBR cerca nella partizione il file **IO.SYS**, a cui cede il controllo; questo a sua volta passa il controllo al file **MSDOS.SYS**, dopodiché passa a leggere il file **CONFIG.SYS**; in quest'ultimo file può essere specificato quale "shell dei comandi" avviare, ovvero quale programma accetterà i comandi inseriti dall'utente tramite tastiera; se non diversamente specificato nel CONFIG.SYS, verrà caricato il file **COMMAND.COM** (se non presente, il PC si bloccherà con un messaggio di errore). A questo punto il sistema è pronto a funzionare. Può però esserci un ulteriore file di configurazione opzionale, l'**AUTOEXEC.BAT**, che permette di avviare automaticamente (AUTOmatically EXECute) alcuni programmi o driver prima di passare il controllo all'utente. In sua assenza, l'interprete dei comandi ci mostrerà direttamente il classico prompt "**C:\>**",.

Sistemi Windows 95/98/ME:
I passi sono gli stessi del caso DOS, fino all'esecuzione dell'AUTOEXEC.BAT, con la differenza che se è presente un file

Struttura dei dischi

Una spiegazione dettagliata sulla struttura fisica e logica dei dischi è disponibile sul sito
www.users.intercom.com/~ranish/part/primer.htm
Un elenco completo di codici delle partizioni è invece su:
http://a2.swlibero.org/~daniele/a2/a221.html

WINBOOT.INI, esso verrà letto al posto del file MSDOS.SYS, che verrà invece del tutto trascurato. Terminata l'esecuzione dell'AUTOEXEC, anziché visualizzare il prompt il sistema si avvierà l'interfaccia grafica Windows; questo significa, in pratica, che fino alla versione 98, **Windows non è un sistema operativo**, ma solo un'interfaccia grafica per il DOS, mentre Windows NT, 2000 e XP sono veri e propri sistemi operativi, avviati al posto del IO.SYS iniziale. Lo dimostra il fatto che il file MSDOS.SYS, in sistemi 95/98/ME, **è solo un file di testo**, contenenti varie opzioni di configurazione, tra cui anche la possibilità di non avviare l'interfaccia grafica, ma restare in ambiente testuale, dove avremo a disposizione il MS-DOS verisone 7.0.
Alla pagina www.penguin.cz/~mhi/mbtmgr/docs/appendix.htm sono spiegate le decine di opzioni disponibili per il file WINBOOT.INI.

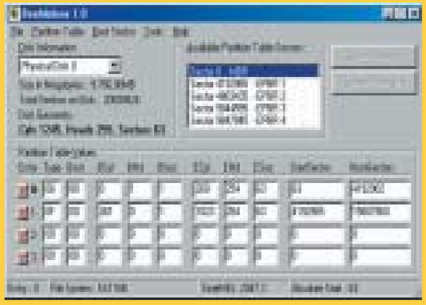
>> Sistemi Windows NT/2000/XP

Invece che al file IO.SYS, il BIOS cede il controllo al file **NTLDR**, che fa passare il processore in modalità protetta a **32 bit** (così può indirizzare fino a 4GB di RAM), e legge dal file BOOT.INI quali sono le modalità di avvio possibili.
Diversamente da Windows 9x/ME, Windows NT permette all'utente di **scegliere quale sistema operativo avviare**, leggendo le possibilità di scelta proprio dal file BOOT.INI.
Se viene scelto NT, verrà avviato **NTDETECT.COM** per il controllo dell'hardware (i dati rilevati verranno scritti poi nella chiave di registro **HKEY_LOCAL_MACHINE\HARDWARE**).
Viene poi caricato (ma non ancora avviato) **NToskrnl.exe** (nella directory \windows\system32\), poi viene caricato **HAL.DLL** (Hardware Abstraction Layer, un modulo che "nasconde" al sistema le varie differenze a livello hardware che esistono tra un computer e l'altro), poi il file "**System**" (che contiene vari dati di configurazione), e successivamente vengono caricati i vari drivers necessari: al caricamento di ognuno corrisponde la comparsa di un puntino sullo schermo. Specificando l'opzione **/sos** nel file **boot.ini**, verrà anche mostrato **il nome del file** caricato. In questa fase i driver non sono ancora inizializzati. A questo punto il controllo viene ceduto a **NToskrnl.exe**, e termina la fase di BOOT, iniziando invece quella di **LOAD**, con la quale vengono avviati i vari programmi utilizzati dal sistema, avviata l'interfaccia grafica e tutto il resto.
Il vostro PC è ora pronto all'uso!
Se invece dal menu di boot selezionate qualcosa di diverso da WindowsNT, il sistema verrà riavviato utilizzando il file **BOOTSECT.DOS** (per default), che contiene appunto il Boot Sector del DOS, o del sistema che esisteva **prima** di installare WindowsNT. Questa scelta di default può essere però modificata, in modo da affidare la procedura di boot a un file contenente **un qualunque boot sector**. Potete trovare dettagli su tutto ciò all'indirizzo www.winplanet.com/winplanet/tutorials/737/1.

Joshua Falken

Utility per smanettoni

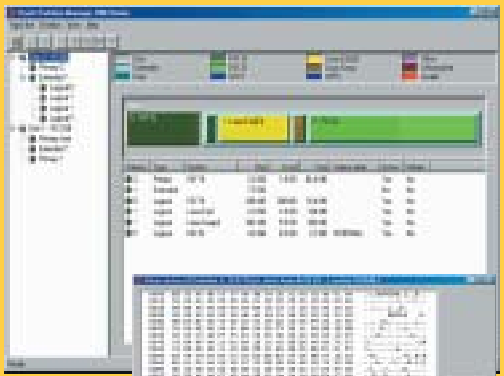
Beeblebrox
Lettura e modifica della tabella delle partizioni (programma sia per windows 98 che per NT). Un programma ottimo ma non più sviluppato
http://students.cs.byu.edu/~codyb/



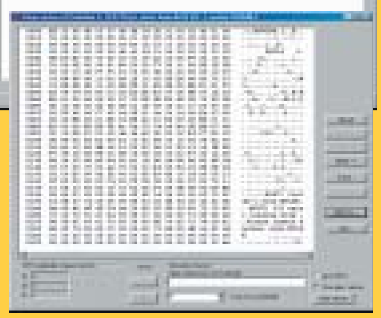
Ranish Partition Manager
Visualizza dettagli sulle partizioni. Programma DOS, ma funziona anche sotto windows.
www.ranish.com/part/

Power Quest Partition Info
Gratuito, visualizza informazioni complete e dettagliate sulle partizioni, gira in ambiente windows (richiede il file
www.direfutbol.com/cpqs/quicksr/PQFF/PQVXD.VXD
o in directory windows\system).
ftp://ftp.powerquest.com/pub/utilities/PARTINFO.ZIP

Power Quest Partition Magic
Programma a pagamento per manipolare le partizioni, anche senza cancellarne i dati.
www.powerqust.com



7tools partition manager
Visualizzatore grafico della struttura delle partizioni: (demo gratuita di programma commerciale) - permette anche di visualizzare e salvare su file i vari boot sector, compreso quello principale (MBR):
www.7tools.com/demo.html



Altri programmi vari per lavorare con le partizioni si trovano su:
www.goodells.net/multiboot/tools.htm

Tutti i dettagli sui codici numerici delle partizioni:
www.win.tue.nl/~aeb/partitions/partition_types-1.html

Programmi per leggere direttamente i settori del disco:
www.geocities.com/SiliconValley/Sector/7256

FASTWEB

Sulla fibra ottica i dati passano sotto forma di impulsi di luce, ma la rete di Fastweb ha anche il suo lato oscuro.

Per uno che ha iniziato le sue scorrerie telematiche con un modem a 1200 bps, l'offerta Fastweb di connettività a 10 Mbit per privati ti mette in uno stato che va molto, molto vicino al Nirvana. Certo, il prezzo non è indifferente, e volendo guardare, per quella cifra uno si aspetterebbe qualche servizio in più (persino i provider free regalano uno spazietto Web, per esempio). La politica di Fastweb, è invece di segno opposto: quando si da tanta banda per un utilizzo domestico, bisogna impedire che qualcuno la sfrutti per offrire servizi che - altrimenti - andrebbero pagati profumatamente.

>> Particolarità della rete

La rete di Fastweb ha quindi alcune limitazioni, la più importante delle quali è che ogni utente domestico non ha a disposizione un indirizzo IP pubblico, nemmeno dinamico. Con un IP pubblico, infatti, sarebbe possibile metter su un server in casa (Web, ma non solo). Ogni utente quindi esce su Internet con l'indirizzo IP del proxy di Fastweb. Uno dei primi tentativi (riusciti) di hackeraggio di Fastweb è consistito quindi nell'individuare un metodo per aggirare questa limitazione. Il metodo individuato da naif (pubblicato su Bfl, Butchered from Inside) si basava sull'utilizzo dell'ftp passivo.

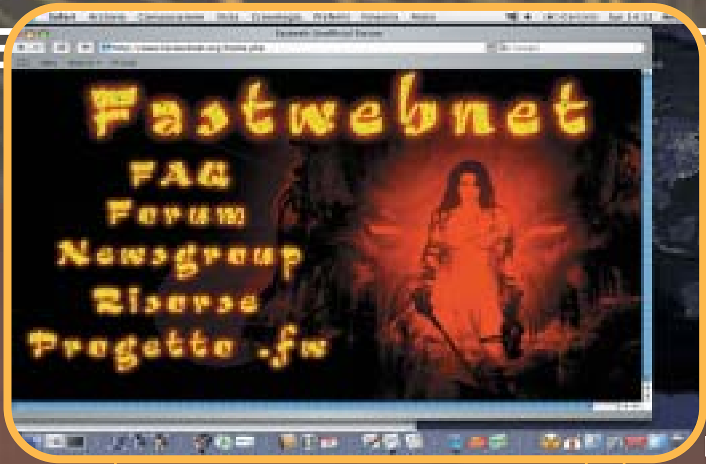
Quando si richiede un file a un server ftp attraverso la modalità passiva, quello che succede è che stiamo dicendo al server di collegarsi al nostro computer e inviare i dati al client. Avete capito bene: la richiesta di trasferimento parte dal server e arriva al client. Ma come fa, se non è possibile contattare direttamente l'IP del client? La soluzione adottata da Fastweb per permettere l'uso di ftp passivo è la Port Address translation: viene aperta sul proxy una porta che, all'interno della rete Fastweb, corrisponde all'IP dell'utente. Quindi, nel momento in cui si fa un trasferimento ftp passivo, c'è una porta aperta, che può essere sfruttata. È stato quindi realizzato un programmino che effettua ripetute connessioni a un server ftp, mantenendo quindi aperta la porta sul proxy. Con un po' di intuito, si ricava l'indirizzo IP pubblico corrispondente al proprio IP privato (che avrà forma IP:porta). Su Bfl, questo metodo è stato pubblicato a scopo di analisi e studio, e l'autore si raccomandava di non impiegarlo solo con server ftp di cui si aveva il controllo, o l'autorizzazione. Purtroppo, invece, molti si sono messi a usare il programmino con server ftp pubblici, tanto che gli amministratori dei server, infastiditi dalle migliaia di connessioni a vuoto, hanno cominciato a bannare tutti gli utenti Fastweb dalla propria rete, con notevole disagio per chi, da Fastweb, voleva per esempio scaricarsi l'ultima Debian.

>> Occhio alle condivisioini

Abbiamo visto che la rete di Fastweb funziona in pratica come una grande LAN connessa a Internet attraverso un proxy, con tutti i rischi che questo comporta: in una LAN infatti diventano molto più semplici molti tipi di attacco. Sniffing, fingerprinting ed esplorazione delle risorse sono solo alcuni dei rischi. All'inizio, addirittura, era possibile vedere tra le proprie Risorse di Rete tutte le condivisioni degli utenti del proprio palazzo o dell'intero



NEWBIE



quartiere. La situazione sembra essere migliorata, perché l'esplorazione delle risorse condivise è stata in qualche modo limitata, ma in realtà l'accesso a tali risorse è ancora possibile. Insomma, non stupitevi più di tanto se vedete comparire dalla vostra stampante un foglio con un documento che non avete mai visto.
La soluzione è abbastanza ovvia: limitate al minimo la condivisione di risorse, e usate un firewall per suddividere le zone sicure (la vostra rete domestica) da quelle insicure (non solo Internet, ma anche tutti gli indirizzi LAN che non appartengano a un vostro computer).
D'altro canto, questa stessa limitazione può consentire di condividere risorse tra due punti anche molto lontani, in modo velocissimo: dovete passare un file molto grande a un vostro amico dall'altra parte della città? Apritegli una condivisione (con password, mi raccomando), dategli il vostro IP, e lui potrà vedere il vostro disco tra le sue risorse di Rete.



>> Il P2P definitivo

Come ogni tipo di comunicazione diretta tra due utenti, anche lo scambio file con i software Peer 2 Peer ha da un lato alcune limitazioni (gli utenti esterni alla rete non riescono a scaricare da un utente Fastweb), ma dall'altro lato quando si scarica da un altro utente Fastweb, le velocità di trasferimento possono sfiorare i 900 Kbyte al secondo: significa scaricare un intero CD in meno di un quarto d'ora.
In realtà, è possibile consentire download dall'esterno, se si imposta l'uso di un proxy; questo però impedisce il download agli utenti interni alla rete.
Visto che le connessioni tra utenti Fastweb vanno così veloci, qualcuno ha pensato di creare server di file sharing riservati a loro. Da molto tempo sono stati creati e vengono mantenuti dei server interni alla rete di Fastweb, attraverso i quali gli utenti possono scambiarsi allegramente file a larga banda. Ne esistono un po' per tutti i sistemi (Open Nap, WinMx, eDonkey, Direct Connect), e basta cercare un po' per trovare una prima lista di indirizzi, da arricchire poi cercando gli aggiornamenti sulla rete P2P stessa.

>> TV e Video

Fastweb distribuisce su fibra ottica anche trasmissioni televisive, che si possono vedere sulla TV con un apparecchio chiamato VideoStation: filmati "on demand" di RaiClick e trasmissioni streaming dei canali di Pay TV (Al momento Sky, prima Tele+ e Stream). Per vedere questi programmi bisogna attivare un ulteriore abbonamento, esattamente come per il satellite.
Peccato però che le trasmissioni di Fastweb non fossero minimamente cifrate: bastava conoscere l'indirizzo giusto di ogni canale (ricavabile osservando un po' quali indirizzi contatta la VideoStation), e si potevano vedere su ogni PC su cui potesse funzionare un programma che permette lo streaming da rete, come VideoLan Client. In pratica, nonostante tutte le menate sulla sicurezza delle schede TV, Seca 2 eccetera, le Pay TV erano visibilissime proprio sulla piattaforma dove, potenzialmente, potevano essere più sicure (non è possibile autenticare una parabola, ma una scheda di rete sì!).

>> Perché tanti problemi?

I problemi di sicurezza di cui abbiamo parlato qui (utilizzo degli Ftp esterni, possibilità di vedere la Pay TV senza pagare) sono stati recentemente risolti, ma erano noti da mesi, se non anni. Eppure risolverli non era poi così difficile. Perché allora Fastweb non li ha sistemati prima? Possibile che non sapessero nulla, quando cercando "Fastweb" su Google tra le pagine italiane, alcuni dei link che citiamo in questo articolo compaiono nella prima pagina?
Non è che, per caso, la presenza di questi "buchi" rendeva più attraente l'offerta di fastweb per certi potenziali utenti? Del resto, i costruttori di decoder e parabole erano ben contenti della diffusione delle schede pirata: gli unici a rimetterci sono infatti le PayTV; tutti gli altri (costruttori, installatori, rivenditori) ci guadagnavano soltanto.

Gino O'Knaus

LINK UTILI

Forum degli utenti FW
www.forum.fastwebnet.org/
www.assitecforum.com/forum2/default.asp?CAT_ID=3
http://forumfastweb.altervista.org/newforum/index.php?act=idx
http://fastsharing.altervista.org/
http://mauryzio.interfree.it/forum/fastland.htm

Faq "ufficiose", realizzate dagli utenti
http://gofastweb.cjb.net/
www.akash.it/pc/fastweb.php

Testi di Butchered from Inside
www.s0ftpj.org/bfi/dev/BFi11-dev-08.tar.gz
www.s0ftpj.org/bfi/online/bfi10/BFi10-13.html
www.s0ftpj.org/bfi/dev/BFi11-dev-12.tar.gz



> Le variabili di shell

Ultima puntata della panormaica sulla Programmazione della shell con GNU/Linux

Nelle prime due puntate di questo mini-corso abbiamo trattato diversi argomenti che ci offrono solide basi per iniziare a programmare con la shell. In questa terza ed ultima puntata analizzeremo le istruzioni iterative, il calcolo aritmetico e le variabili di shell, argomenti che necessitano della lettura delle prime due puntate per essere compresi.

>> Variabili di shell

Le **variabili di shell** sono delle variabili speciali che la shell crea e utilizza durante il suo funzionamento. Esse sono molto utili poiché consentono al programmatore di **ottenere alcuni dati sul sistema, sull'utente, sul funzionamento della shell** e così via.

ECCO ALCUNE VARIABILI DEFINITE DIRETTAMENTE DALLA SHELL:

PPID Il PID del processo genitore della shell
PWD Il percorso dell'attuale directory di lavoro
OLDPWD Il percorso della precedente directory di lavoro
REPLY L'output del comando read in assenza di input
UID User ID dell'utente corrente
EUID User ID effettivo dell'utente corrente
GROUPS Array dei GID di cui l'utente è membro
BASH Il nome utilizzato per avviare questa istanza di bash
BASH_VERSION La versione di questa istanza di bash
SHLVL Variabile incrementata di uno per ogni istanza di bash avviata
RANDOM Un numero intero casuale
SECONDS Numero di secondi trascorsi dalla chiamata della shell
LINENO Numero della linea corrente in uno script
HISTCMD Numero del comando corrente nella storia della shell
OPTARG L'ultimo argomento opzione processato da getopts
OPTIND L'indice del prossimo argomento che getopts processerà
HOSTTYPE Il tipo di macchina su cui bash sta girando
OSTTYPE Il sistema operativo su cui bash sta girando
MACHTYPE Architettura e sistema operativo della macchina su cui bash sta girando

ECCO ALCUNE VARIABILI DEFINIBILI, OLTRE CHE DALLA SHELL, ANCHE DALL'UTENTE:

IFS Internal Field Separator; viene usato nella suddivisione in parole e di default corrsiponde a "<spazio><tab><nuovalinea>"
PATH Percorso in cui la shell cerca i comandi da eseguire
HOME La home directory dell'utente corrente
CDPATH Il percorso di ricerca per il comando CD
ENV File di configurazione per l'esecuzione di script
MAIL File contenente la posta elettronica dell'utente
MAILPATH La directory dei file di posta elettronica dell'utente
MAILCHECK Intervallo tra un controllo della posta ed un altro
PS1 L'invito primario
PS2 L'invito secondario
PS3 L'invito del costrutto select
PS4 Parametro usato durante un trace di esecuzione
HISTSIZE Il numero di comandi da memorizzare nella storia della shell
HISTFILE Il nome del file su cui memorizzare la storia della shell
HISTFILESIZE Il numero di linee massime occupabili nel file della storia della shell
TMOUT Tempo di attesa massimo (timeout)
PROMPT_COMMAND Comando da eseguire prima di mostrare un nuovo prompt

Per maggiori informazioni sulle variabili di shell vi invito a leggere la pagina **man** di **bash**.

>> Calcolo aritmetico

Come per ogni linguaggio di programmazione che si rispetti, anche la bash offre degli strumenti per effettuare **operazioni aritmetiche di base**. Ecco l'elenco delle operazioni supportate :

? + Meno e più unari
! ~ Negazione logica e "bit a bit"
*** / %** Moltiplicazione, divisione, modulo (resto)
+ ? Addizione, sottrazione
<< **>** Shift "bit a bit" a sinistra e a destra
<= **>=** < **>** Confronti
== != Uguaglianza e disuaglianza
& AND "bit a bit"
^ OR esclusivo "bit a bit"
| OR "bit a bit"
&& AND logico
|| OR logico
= *= /= %= += ?= <<= **>= &= ^= |=** Assegnamento

Le **operazioni** si effettuano all'interno di **doppie parentesi tonde** o tra **parentesi quadre** precedute dal simbolo **$**.

Ecco uno script che costituisce una calcolatrice di base per numeri interi:

```
#!/bin/bash
# Calcolatrice per numeri interi
echo "Calcolatrice per numeri interi"
echo "Operazioni supportate : + - * /"
echo -n "Primo valore: "
read PRIMO_VALORE
echo -n "Secondo valore: "
read SECONDO_VALORE
echo -n "Operazione: "
read OPERAZIONE
case $OPERAZIONE in
        "+") RISULTATO=$[$PRIMO_VALORE+$SECONDO_VALORE]
;;
        "-") RISULTATO=$[$PRIMO_VALORE-$SECONDO_VALORE]
;;
        "*") RISULTATO=$[$PRIMO_VALORE*$SECONDO_VALORE]
;;
        "/") RISULTATO=$[$PRIMO_VALORE/$SECONDO_VALORE]
&& RESTO=$[$PRIMO_VALORE%$SECONDO_VALORE] && echo
"Resto: $RESTO" ;;
esac
echo "Risultato: $RISULTATO"
```

>> Istruzioni iterative

Le **istruzioni iterative** costituiscono un particolare tipo di istruzioni che eseguono ciclicamente delle operazioni. Oltre al costutto select che abbiamo analizzato nella puntata precedente, le istruzioni iterative supportate dalla bash sono **for**, **while** e **until**.
L'istruzione **for** esegue una scansione all'interno di una **lista** e **mostra in sequenza** gli argomenti che gli sono stati forniti. Analizziamo insieme questo esempio:

```
#!/bin/bash
# Riproduttore di file Ogg Vorbis
echo "Riproduttore di file Ogg Vorbis"
if [ $# = 0 ]
then
echo "Devi fornire al programma almeno il nome di un
file Ogg Vorbis"
exit
else
for PARAMETRO
do
ogg123 "$PARAMETRO"
done
echo "Riproduzione completata"
fi
```

In questo caso l'istruzione for è stata utilizzata per creare un piccolo **riproduttore di file Ogg Vorbis** servendosi di ogg123. La sintassi di for è molto semplice: si definisce una **variabile** che assumerà ogni volta il valore di uno degli argomenti ottenuti attraverso **in** e una **lista** (se omessi, come in questo caso, si fa riferimento a tutti i parametri posizionali a partire dal primo), mentre le operazioni da eseguire vengono racchiuse tra **do** e **done**.
L'istruzione **while** esegue un'operazione fino a quando una condizione risulta sempre vera. Ecco un esempio:

```
#!/bin/bash
# Calcolo la potenza di un numero intero positivo con
while
echo "Programma per il calcolo delle potenze di numeri
interi"
echo -n "Base: "
read BASE
echo -n "Esponente: "
read ESPONENTE
if [ $BASE = "0" ]
then
RISULTATO="0"
elif [ $ESPONENTE = "0" ]
then
RISULTATO="0"
elif [ $BASE = "1" ]
then
RISULTATO=$BASE
elif [ $ESPONENTE = "1" ]
then
RISULTATO=$BASE
else
RISULTATO=$(($BASE*$BASE))
ESPONENTE=$(($ESPONENTE-2))
while [ $ESPONENTE != 0 ]
do
RISULTATO=$(($RISULTATO*$BASE))
ESPONENTE=$(($ESPONENTE-1))
done
fi
echo "Il risultato è: $RISULTATO"
```

La **condizione** va espressa tra **parentesi quadre**, mentre le istruzioni da eseguire vanno racchiuse tra **do** e **done**.

L'istruzione **until** invece svolge il compito opposto di while: esegue delle istruzioni fino a quando la condizione espressa risulta sempre falsa. Ecco la parte di codice relativa al calcolo di potenze con while riscritta utilizzando until:

```
until [ $ESPONENTE = 0 ]
do
RISULTATO=$(($RISULTATO*$BASE))
ESPONENTE=$(($ESPONENTE-1))
done
```

L'istruzione until ha la stessa sintassi di while.

>> Conclusione

Il nostro mini-corso di programmazione della shell con GNU/Linux termina qui. Spero di essere stato abbastanza chiaro nell'esposizione dei concetti e di avervi fornito tutti gli elementi necessari per realizzare solidi script di shell.
Per dubbi, suggerimenti e critiche potete inviarmi una e-mail all'indirizzo specificato in basso.
Per apprendere ulteriori nozioni relative alla programmazione di shell con GNU/Linux potete consultare il box Documentazione presente in quest'articolo.
Vi auguro una felice programmazione con GNU/Linux :)

pctips

HACKER JOURNAL

Anno 2 - N. 38
20 Novembre - 4 Dicembre 2003

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
grand@hackerjournal.it, Il Coccia, Gualtiero Bismark.it, Tronconi, Ana Esteban, Marco Bianchi, Edoardo Bracaglia, Polao Capobussi, Lucio Bragagnolo, Amedeu Bruguès, Gregory Peron

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Roto 2000

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.
Direttore responsabile - Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE
Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. **redazione@hackerjournal.it**

hack·er (hăk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

HACK'N'ROLL

Da questo mese viene pubblicata anche in Italia la rivista Rolling Stone, probabilmente la più antica e importante pubblicazione Rock americana. A sfogliarla, però, non si può non avere una sensazione strana. La parte editoriale prende; in molte parti è ruvida come dovrebbe. La pubblicità, invece, è quella che ci si aspetta di trovare in una rivista da parrucchiere maschile di tendenza: stilisti, profumi, auto di lusso e un po' di gagdet hi-tech.

Non so voi, ma quando vado a un concerto, l'unica mia preoccupazione in fatto di vestiti è che non deve dispiacermi troppo se i pantaloni si macchiano di fango fino alla cintura, o se la maglietta si strappa mentre sto pogando. E le scarpe devono essere abbastanza comode da farmi stare in piedi finché ne ho voglia.

Insomma, in bocca rimane uno strano sapore metallico addolcito da troppo miele, una specie di incongruenza, una contraddizione di fondo. Che traspare anche da alcune pubblicità. Una di queste mi ha colpito in particolare. Una pagina del super gestore Telefonico Italiano che pubblicizzava il suo servizio Adsl ricaricabile (che qui chiamerò celiA). Il titolo cerca di stare a suo agio sulla rivista: "Card Rock", e la frase a effetto non è da meno: "Non senti altro che MP3? Usa l'Adsl quando ce n'è un buon motivo".

Ora, avete anche voi la sensazione che una grande azienda multinazionale sta cercando di stimolare i suoi potenziali clienti ad acquistare un suo servizio per compiere un'azione quanto meno discutibile?

Altre multinazionali non si trovano in una situazione migliore: c'è un colosso dell'elettronica che ha anche varie etichette discografiche (visto che sono in vena, lo chiamerò Nyso), e mentre una sua mano produce dischi e si batte con tutti i mezzi perché non vengano copiati, prestati, ascoltati da più di cinque persone eccetera, con l'altra mano produce e vende masterizzatori e supporti di ogni tipo.

La cultura Rock e quella dell'hacking hanno molto in comune: quel senso di appartenenza a una comunità, il gusto per per l'estremo, le sfide ai margini della legalità, e un sano senso di ribellione. E anche dalle nostre parti c'è qualcuno pronto a usare questi elementi per guadagnarci.

Stanno infatti cominciando a sorgere aziende che dicono di praticare l'"hacking etico" per cavalcare un filone che ora va di moda, ma con l'hacking non hanno nulla a che fare. Oltre ovviamente alle altre aziende di sicurezza tradizionali, per le quali l'hacker è solo uno spauracchio da agitare davanti ai clienti per terrorizzarli e vendergli i suoi prodotti.

L'argomento è complesso, delicato, e non può esaurirsi in mezza paginetta. Ne parliamo infatti nell'articolo alle pagine 10-13, tenendo ben presente anche che accanto a questi, ci sono anche alcuni hacker che hanno sfruttato le proprie conoscenze per inventarsi un lavoro senza per questo abbandonare lo spirito originale, e infatti continuano a rendere disponibili i propri software e i propri studi.

grand@hackerjournal.it

PS: in ogni caso, benvenuta Rolling Stone ;-)

HOT!

GLI OCCHI A MANDORLA DELLA CENSURA



Il Grande Fratello del Ministero della Cultura cinese ha puntato il suo occhio inquisitore sugli Internet Cafè della nazione. Non solo tutti i punti di accesso pubblico alla Rete saranno obbligati a installare software di controllo per monitorare le attività dei clienti. Pare anche che la licenza di apertura di esercizi verrà d'ora in poi concessa esclusivamente a grandi catene controllate dallo Stato. La situazione incresciosa è stata denunciata da Reporter Senza Frontiere (http://www.rsf.org/), organizzazione che da anni si batte per la libertà di informazione nel mondo.

LINEA DURA PER TELIA



Telia, uno dei più grandi Internet Service Providers svedesi ha deciso di bloccare i computer di tutti coloro che inviano spamming tramite i suoi server. I computer bloccati principalmente sono quelli infestati da trojans che spediscono all'impazzata centinaia di messaggi indesiderati. Immaginiamo la gioia degli utenti: infetti e mazziati, ehm… inchiodati. Telia assicura comunque di offrire assistenza ai malcapitati, aiutandoli a rimuovere il problema il più velocemente possibile.

MA…CHIEDERE IL PERMESSO?

La botta di iniziativa di AOL ha lasciato tutti quanti stupefatti e parecchio contrariati. Senza minimamente interpellare i suoi abbonati, il colosso americano ha infatti deciso di disabilitare Windows Messenger. Il servizio, che nulla ha a che vedere con il client di messaggistica istantanea, è vero, costituiva un canale privilegiato per lo spamming, nonché un punto di possibile vulnerabilità per il sistema. Ma non si capisce come AOL si possa essere presa tale ingiustificata e ingiustificabile libertà. Libertà che, diciamocela tutta, a un ragazzino o hacker qualunque sarebbe costata indagini, diffide, sanzioni e quant'altro. AOL si difende dalle accuse come niente fosse, dicendo che il servizio è per lo più sconosciuto agli utenti, che è riattivabile con un clic del mouse e che ha avuto accordi sulla faccenda con il big di Redmond. Animata da tante buone intenzioni, forse AOL non si rende conto del paradosso. Combattere l'intrusione con… un'intrusione non richiesta. Ma del resto c'è anche chi pensa di fermare le guerre con altre guerre. Deve essere così che va il mondo.



TRENI DEL FUTURO DISAGI DEL PRESENTE?

Carrozze attrezzate per connessioni wi-fi, passeggeri mollemente adagiati che ingannano il tempo guardando la TV on demand, alacri omini incravattati che trasformano il viaggio in treno in un'occasione per lavorare ancora di più e meglio. Ma dove siamo? In un film ambientato nel futuro o tra i fotogrammi dell'incubo di un qualche manager malato di efficientismo e di tecnologismo? Macchè. Siamo a Genova dove pochi giorni fa Trenitalia ha presentato un nuovo modello di treno del futuro. Il progetto si chiama Fifth (Fast Internet For Fast Train Host), è realizzato in collaborazione con Alenia Spazio e prevede l'allestimento di spazi tecnologicamente attrezzati sui treni di lunga percorrenza. Le sperimentazioni avranno luogo per tutto il 2004 su treni speciali. Dall'anno successivo i servizi saranno disponibili sugli Eurostar ed entro il 2005 anche sugli Intercity. Che dire, siamo fieri di essere italiani, di essere al passo con l'Europa e di essere promotori di servizi tanto all'avanguardia. Anche se qualche volta ci basterebbe che i convogli di Trenitalia giungessero puntuali, non imballati come una discoteca la notte di capodanno, non ammorbati e appiccicosi come la stessa discoteca la mattina dopo, che fossero tiepidi d'inverno e almeno un po' freschi d'estate. È chiedere troppo?



A OGNUNO LA SUA PROTEZIONE

I bambini si sa, hanno l'occhio lungo e a volte curiosità un po' troppo pruriginose per la loro giovane età. Per i genitori preoccupati della sicurezza online dei loro figli, Telecom lancia Alice Family. Si tratta di un'offerta di abbonamento ADSL che prevede quattro caselle di posta e quattro accessi alla Rete indipendenti. Grazie a Parental Control, ogni accesso potrà collegarsi a Internet con un diverso grado di protezione, tutelando così i più piccoli da visioni e contenuti non adatti, anche quando mamma e papà non sono in casa. Fino al 31 dicembre l'attivazione di Alice Family sarà gratuita. Dopo di che costerà 2 euro al bimestre.
Per informazioni: www.aliceadsl.it.



MA GUARDA CHE SORPRESA

Metti un giorno di essere online sulla tua scheda abbonato Sky,. Metti di essere annoiato e di cincischiare con i numerelli dell'url. Metti che, cambia una cifra qua e una là, e guarda un po' cosa accade. Ti si visualizza in tutto il suo splendore la scheda di un altro abbonato. Con tanto di nome, cognome, indirizzo e dati personali. Sembra impossibile, dato che i server di Sky sono di tipo sicuro. Eppure è successo ad alcune persone che poi hanno segnalato l'accaduto a Punto Informatico. Per fortuna la pagina Web che permette questo tipo di accesso non è facilmente raggiungibile dal sito dell'operatore satellitare. Il problema risiede infatti in una macchina di servizio utilizzata dalla rete di dealer Sky e non del server dove si trova il sito dell'operatore. Sky è stata avvertita, dunque si suppone che a breve di questo imbarazzante inconveniente non vi sia più traccia.



OPERAZIONE CATARTICA



Sì, la buona riuscita dell'operazione della guardia di finanza contro il worm Zelig è stata una sorta di purificazione liberatoria. Soprattutto per i portafogli a rischio di molti internettari. Nei giorni tra il 24 e il 25 ottobre scorsi, si è diffuso un messaggio di posta elettronica apparentemente innocuo che invitava a visitare un sito dove avremmo trovato un salvaschermo con "messaggi catartici", le ormai note perle di saggezza di Flavio Oreglio di Zelig. Una volta raggiunta la home page indicata, avviare il download era un attimo. Inutile dire che si trattava di una truffa che dirottava la nostra connessione telefonica su un numero da 1,80 euro al minuto. Per fortuna il pericolo è scampato. L'organizzatore della truffa, un commerciante di pelli di Pisa domiciliato a Caracas, è già stato fermato dalle forze dell'ordine. Stiano tranquilli tutti coloro che hanno ceduto alla tentazione del clic. Grazie al tempestivo intervento della GdF, non riceveranno le tanto temute, e per nulla catartiche, bollette astronomiche.

ALLO SPAMMER! ALLO SPAMMER!

Le vie dello spamming sono davvero infinite. Gira voce che cominci a diffondersi questa piaga anche via Bluetooth. Il fenomeno si chiama bluejacking e per ora sembra sia soltanto la bravata di qualche buontempone. Ma non fatichiamo pensare che spammers seri prima o poi possano approfittare della possibilità di inviare messaggi via Bluetooth tra dispositivi accesi nel raggio di pochi metri . Ci immaginiamo eserciti di mercenari, che travestiti da uomini d'affari sparano messaggi indesiderati, sui treni, in metropolitana, alla stazione, negli uffici. Che succederà a quel punto? Diffidentissimi, copriremo telefoni, computer e palmari con gli astucci, come quando a scuola non volevamo ci copiassero. E al minimo sospetto urleremo impalcabili "allo spammer! allo spammer! prendetelo!".



HOT!

C'È SEMPRE UNA PRIMA VOLTA



La prima volta non si scorda mai. Anche quando si tratta di vincere una causa anti spam. Per la California l'evento è di qualche giorno fa. La causa è costata ben due milioni di dollari di multa a una azienda di marketing che ha inviato milioni di mail non richieste. Nei messaggi si trovavano consigli su come realizzare mail pubblicitarie e una quantità spropositata di indirizzi di posta elettronica. Oltre ricevere la multa, i responsabili dell'operazione marketing sono stati diffidati dal gestire e amministrare affari che riguardino la pubblicità in Rete per i prossimi dieci anni.

OPEN SOURCE NO PROBLEM

Le Amministrazioni pubbliche che vogliono passare da software proprietari a software open source, prendano nota del sito dell'Unione Europea, http://europa.eu.int. Qui si trovano informazioni sui diversi prodotti open source e una tabella per calcolare quanto si risparmia passando da una formula all'altra. Il documento, redatto da esperti nel settore di tutta Europa, è costantemente aggiornato.

LA VERITÀ È VICINA

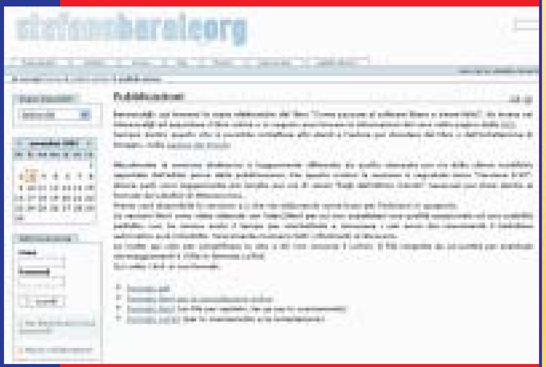
POLIZIA di Stato

Si è finalmente aperta l'inchiesta della Polizia Postale e delle Comunicazioni sulla truffa anti eBay. Il raggiro riguarda un messaggio fasullo che cerca di convincere gli iscritti a eBay a inviare i dati personali, compresi quelli della carta di credito. Al momento le indagini sono ancora in corso e non si sa né chi abbia architettato il piano, né quante persone siano cadute nella trappola dei truffatori. Naturalmente eBay è assolutamente estranea alla faccenda. Anzi, ricorda che non avrebbe ragione alcuna di richiedere informazioni del genere ai suoi iscritti.

NEWS

HOT!

PER SAPERNE DI PIÙ



Se ancora l'open source non ci ha convinti del tutto e aspettiamo quell'argomentazione in più per liberarci dai vincoli del software proprietario, proviamo a dare un'occhiata a questo libro. Costa 10 Euro e si chiama "Come passare al software libero e vivere felici - Manuale di autoliberazione informatica". Tra le sue pagine troveremo non solo teoria ma anche tanta pratica e spiegazioni tecniche. Sul sito dell'autore, www.stefanobarale.org è disponibile anche la versione elettronica della pubblicazione.

MCDONALD'S CONNECTION

Nessuno resiste più alla voglia di wi-fi, nemmeno Mc Donald. Nostro Signore degli Hamburger sta prendendo accordi con alcuni dei più noti fornitori di tecnologia wi-fi per dotarsi delle infrastrutture necessarie al collegamento wireless a banda larga. Così tra una patatina e l'altra i clienti potranno ingannare il tempo sfrecciando da un sito all'altro. E chissà mai che pur di navigare a velocità tanto golose, gli avventori siano disposti a ingollarsi molti più panini annegati nel ketchup di quanto fame o istinto di autoconservazione non suggeriscano.



NON SIAMO CATTIVI, SIAMO SOLO CURIOSI.



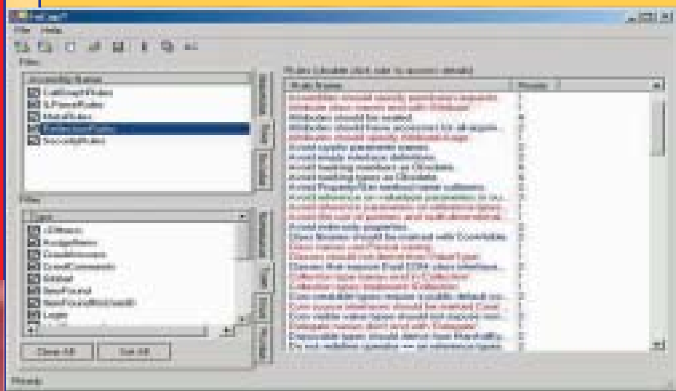
Hacker e Cracker. Due sole lettere di differenza per indicare categorie di persone tra cui c'è un abisso. Da una parte coloro che sono appassionati di tecnologie informatiche e che cercano di carpirne tutti i segreti possibili e immaginabili, restando nel lecito. Dall'altra persone a cui non basta il piacere della conoscenza, ma per sentirsi soddisfatti devono combinare malefatte informatiche a danno di terzi. Da una parte gli hacker dall'altra i cracker. Da una parte i buoni dall'altra i cattivi. Ci tengono a marcare questa netta divisione gli hacker, che per difendere la propria cultura e dignità di categoria, hanno anche fondato il progetto HANC. Acronimo di Hackers Are Not Crackers, o Hackers Are Not Criminals se preferiamo, questo manifesto sottolinea che gli hacker che non sono affatto pirati informatici come invece il dipingono i media, probabilmente per superficialità e ignoranza in materia. Chi volesse dare un'occhiata e dare il proprio contributo a diffondere la cultura hacker si può collegare al sito http://www.hancproject.org/.

PALMA D'ORO A NAPOLI



Si dice che San Gennaro protegga sempre i napoletani. Ma ci sa che questa volta il Santo nulla abbia potuto, per togliere alcuni suoi cittadini dalle grinfie delle forze dell'ordine. Tanto meglio, perché si trattava di persone disoneste che frodavano la legge sul diritto d'autore duplicando CD audio e software da rivendere sul mercato nero. Il bliz che la Guardia di Finanza ha portato a termine a Napoli negli scorsi giorni non ha precedenti. Sono stati individuati e messi sotto sequestro diversi laboratori altamente tecnologici con una capacità di duplicazione di circa tremila copie illegali all'ora. Nove le persone arrestate e trecentomila euro il valore della merce ritirata. All'operazione spetta la palma d'oro del più imponente sequestro mondiale di attrezzatura in termini di qualità e valore. Che dire, Napule è sempre Napule. Esagerata e grandiosa, nel bene e nel male.

L'UNIONE FA LA FORZA, SPERIAMO



Intorno a Bill Gates soffiano forti venti di apertura. Microsoft ha infatti annunciato di voler condividere con gli sviluppatori strumenti interni utilizzati per creare prodotti più sicuri e affidabili. Certo dato il numero di bug che esce dagli edifici di Redmond, c'è quasi da augurarsi che la condivisione di know how non superi certi limiti. Ma non vorremmo essere troppo cattivi. Vogliamo invece sperare che la collaborazione tra le persone possa dare i suoi buoni frutti come sempre. Tra le utility rilasciate ci sono Prefix e Prefast, due tool diagnostici che analizzano il codice sorgente in formato testo per trovare bachi nel codice C++. C'è un utilissimo programma che mette a disposizione degli sviluppatori uno schema su errori e vulnerabilità cui sono soggette le applicazioni già al momento della progettazione. Infine c'è FxCop un tool direttamente scaricabile all'indirizzo http://www.gotdotnet.com/team/fxcop/ che permette di evidenziare eventuali falle nella programmazione e controlla che il codice sviluppato sul modello MS.NET sia conforme alle linee guida del MS.NET Framework.

L'ULTIMA MAGIA DI HARRY POTTER



Nel carnet delle possibili magie del simpatico maghetto occhialuto ci deve essere anche quella di far sparire i siti. Se no non si spiega come mai sia stato parzialmente oscurato il sito del radicale Pietrosanti, promotore di un'iniziativa che riguarda, guarda caso, proprio Harry Potter. Insieme a un gruppo di non vedenti Prietrosanti sta organizzando una prossima vendita online della versione digitale dell'ultimo episodio della saga di Harry Potter a soli 4,8 euro. Prezzo che andrebbe a coprire i soli costi dei diritti d'autore. Si capisce che la faccenda abbia scatenato le ire degli editori, (Salani), che hanno promesso guerra e vendetta per una simile onta. E soprattutto per le presunte perdite economiche che tale vendita online comporterebbe. Quello che non si capisce è perché oscurare il sito di Pietrosanti, visto che non contiene nessun tipo di materiale illegale. A meno che non si consideri illegale la promozione dell'iniziativa e le ragioni che la giustificano. Ancora di meno si capisce come mai da uno dei due siti di Pietrosanti, www. pietrosanti.org invece sia ancora possibile scaricare la versione elettronica di Delitto e Castigo di Dostoevskji. La risposta viene da sé, ed è di sette lettere: censura. La guerra tra le due parti si preannuncia aspra e cruenta. Salani giura di trascinare Pietrosanti in tribunale qualora la vendita online abbia inizio. Pietrosanti e discepoli promettono che il libro in versione digitale verrà comunque distribuito. Attendiamo ansiosi gli sviluppi della contesa.

CARTUCCE IN LIBERTÀ



Forse non tutti sanno che cosa ci stanno a fare i chip sulle cartucce delle stampanti. Per protezione. Trattandosi di dispositivi protetti dal copyright, i chip hanno come unico scopo di impedire la ricarica delle cartucce ed evitare che produttori non autorizzati ne realizzino di compatibili. O meglio, così credevano i big delle cartucce fino a poco tempo fa. Ora una sentenza negli Stati Uniti ha cambiato le carte in tavola. Nel 2002, sicura di vincere, Lexmark ha fatto causa alla società SCC per avere creato cartucce compatibili che riproducevano il funzionamento dei chip Lexmark. Invece il tribunale ha dato ragione alla SCC. C'è infatti una sezione del DMCA, Digital Millennium Copyright Act, che permette alle aziende di sviluppare software allo scopo di rigenerare cartucce di toner e stampanti. La SCC pertanto potrà tranquillamente vendere chips sostitutivi da usare con le vecchie cartucce Lexmark.

LINUX IN DIRITTURA D'ARRIVO



Linus Torvalds & C. l'hanno definita "una significativa pietra miliare". Sarà anche che ogni scarrafone è bello a mamma sua. Ma questa volta il giudizio è obiettivo. Pare che la versione 2.6 del kernel di Linux potrebbe essere la penultima prima della versione finale. Già qualche settimana fa Torvalds aveva assicurato che nelle release non ci sarebbero state altre modifiche che non riguardassero strettamente la correzione di problemi di stabilità del kernel. Il consorzio in cui Torvalds e collaboratori ha esortato fornitori di sistemi, venditori indipendenti di software e clienti di Linux, a provare e verificare la nuova versione 2.6.0-test9 per prepararsi "alla prossima production release di Linux".

HOT!

CHI VA PIANO VA LONTANO?



Per alcune persone downloadare patch dal sito Microsoft è come controllare la posta elettronica. Si va sul server quando capita durante il giorno e si checka. Qualcosa da scaricare c'è sempre. Adesso però Microsoft cambia musica. Gli aggiornamenti arrivano solo una volta al mese. Per dare il tempo agli sviluppatori di risolvere il problema come si deve e non fare brutte figure, come è successo in passato. E se c'è in giro un bug, calma e gesso. Peggio per chi se lo deve pappare. Non si morirà mica ad aspettare una trentina di giorni, no? Il concetto presto e bene, pare che a Redmond non sia ancora giunto. Qualcuno glie lo vuole spiegare?

PILOTI SIMULATI A MILANO

MILANO FLIGHT SIMULATOR SHOW 2003 22/23 NOVEMBRE

Il 22 e il 23 Novembre, presso il Parco Esposizioni di Novegro, a due passi dall'aereoporto di Milano Linate, si terrà il "Milano Flight Simulator Show 2003", una manifestazione tutta dedicata al volo simulato. Oltre agli stand degli espositori (produttori e distributori di hardware e software attinente al tema), e delle varie associazioni di utenti e giocatori, ci sarà uno spazio dedicato a convegni, seminari e presentazioni di sessioni di volo. Se siete appassionati di volo simulato, buttatevi in picchiata su Novegro (tra l'altro, se il vostro simulatore di volo ha una mappa dell'aereoporto di Linate, potete farci anche una ricognizione simulata prima della visita vera e propria).
Per info: http://www.takeoffonline.it